Sistema de prueba de vida para login biométrico usando modelos de machine learning

Cáceres Erraez, Cristóbal Alejandro

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

Msc. Delgado Rodríguez, Ramiro Nanac

24 de agosto de 2022

Trabajo_Titulacion_Caceres_Cristobal_VF_REV_RD.doc

Scanned on: 15:12 August 16, 2022 UTC

Identical Words	355
Words with Minor Changes	67
Paraphrased Words	204
Omitted Words	0

ING. RAMIRO DELGADO, PhD

Departamento de Ciencias de la Computación
Carrera de Ingeniería de Sistemas e Informática

Certificación

Certifico que el trabajo de titulación, "**Sistema de prueba de vida para login biométrico usando modelos de machine learning**" fue realizado por el señor **Cáceres Erraez, Cristóbal Alejandro;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 24 de agosto de 2022

Firma:

Firmado electrónicamente por:
RAMIRO NANAC
DELGADO
RODRIGUEZ

Msc. Delgado Rodríguez, Ramiro Nanac

C.C.: 1707019178

Departamento de Ciencias de la Computación
Carrera de Ingeniería de Sistemas e Informática

Responsabilidad de Autoría

Yo, **Cáceres Erraez, Cristóbal Alejandro**, con cédula de ciudadanía n°1720005550, declaro que el contenido, ideas y criterios del trabajo de titulación: **"Sistema de prueba de vida para login biométrico usando modelos de machine learning"** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 24 de agosto de 2022

Firma:

Cáceres Erraez, Cristóbal Alejandro

C.C.: 1720005550

Departamento de Ciencias de la Computación
Carrera de Ingeniería de Sistemas e Informática

Autorización de Publicación

Yo, **Cáceres Erraez, Cristóbal Alejandro,** con cédula de ciudadanía n°1720005550 autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Sistema de prueba de vida para login biométrico usando modelos de machine learning"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 24 de agosto de 2022

Firma:

.....

Cáceres Erraez, Cristóbal Alejandro

C.C.: 1720005550

Dedicatoria

El presente trabajo de titulación está dedicado a:

Mis padres, quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un meta más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mi hija, quien merece tener un padre que influya un ejemplo positivo de constancia y dedicación para cumplir todas las metas que planteemos en nuestras vidas.

A mi novia por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias, porque con sus oraciones, consejos y palabras de aliento hizo de mí una mejor persona y de una u otra forma me acompaña en todos mis sueños y metas.

Agradecimientos

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.

Mi profundo agradecimiento a todas las autoridades y personal que hacen a Kruger, por confiar en mí, abrirme las puertas y permitirme realizar todo el proceso investigativo.

De igual manera mis agradecimientos a la Universidad de las Fuerzas Armadas ESPE, a todo el departamento de Ciencias de la Computación, a mis profesores en especial a Ramiro Delgado y Diego Marcillo quienes con la enseñanza de sus valiosos conocimientos hicieron que pueda crecer día a día como profesional, gracias a cada uno de ustedes por su paciencia, dedicación, apoyo incondicional y amistad.

Contenido

CopyLeaks 2

Certificación 3

Responsabilidad de Autoría 4

Autorización de Publicación 5

Dedicatoria 6

Agradecimientos 7

Contenido 8

Índice de Tablas 11

Índice de Figuras 12

Resumen 14

Palabras clave: prueba de vida, inteligencia artificial, reconocimiento facial 14

Abstract 15

Keywords: proof of life, artificial intelligence, facial recognition 15

Capítulo I 16

Introducción 16

Antecedentes 16

Problemática 17

Objetivos 17

Objetivo General 17

Objetivos Específicos 18

Justificación 18

Alcance 18
Marco teórico 19
Docker 19
Python 20
HTML, CSS, JS 20
Inteligencia artificial 20
Prueba de vida 41
Proveedor de identidades y accesos 44
Metodología de investigación 47
Capitulo II 50
Diseño del sistema 50
Problemática y modelo de solución 54
Especificación de protocolos de comunicación 55
Arquitectura del sistema de prueba de vida 55
Módulo de banco de preguntas (challenge_bank) 57
Extender funcionalidades de Keycloak 59
Capítulo III 60
Implementación y pruebas 60
Implementación de los modelos 60
Implementación del banco de preguntas 61
Evaluación de resultados 62
Capítulo IV 66
Conclusiones y líneas de trabajo futuro 66
Conclusiones 66

Recomendaciones 66

Bibliografía 67

Índice de Tablas

Tabla 1 *Comparación entre Inteligencias artificiales Débiles y Fuertes* 24

Tabla 2 *Ejemplos de Capacidades de las Inteligencias artificiales y sus campos de estudio* 25

Tabla 3 *Tipos de artefactos utilizados en la suplantación de identidades* 43

Tabla 4 *Tipos de derivación utilizados en la suplantación de identidades* 44

Tabla 5 *Pasos del método científico experimental* 48

Tabla 6 *Tareas involucradas en la solución propuesta* 50

Tabla 7 *Modelos utilizados en el banco de preguntas* 58

Tabla 8 *Resultados de cada modelo de inteligencia artificial de manera individual* 60

Índice de Figuras

Figura 1 *Mapa de la Inteligencia Artificial* 21

Figura 2 *Elementos que conforman una cara* 27

Figura 3 *Ejemplo de conceptualización de las redes neuronales en diferentes capas* 28

Figura 4 *Diagrama de las redes neuronales* 29

Figura 5 *Estimulación de neuronas con patrones* 31

Figura 6 *Evaluación del diseño de una CCN para la detección de números escritos en cheques bancarios* 32

Figura 7 *Ejemplo de convolución con dos filtros de 3x3 en una imagen RGB de 5x5* 33

Figura 8 *El kernel que se aplica para producir el resultado intermedio más alto para el mapa de activación* 34

Figura 9 *Ejemplo de una red convolucional estándar* 35

Figura 10 *Ejemplo de filtros que detectan patrones complejos a medida que se realizan las convoluciones en cada capa* 36

Figura 11 *Arquitectura de una Red neuronal Convolucional* 37

Figura 12 *Pasos para el entrenamiento de un clasificador de imágenes* 41

Figura 13 *Liveness Detection es una IA que determina si una computadora está interactuando con un ser humano vivo* 42

Figura 14 *Flujo genérico de Keycloak* 45

Figura 15 *Proceso de login con keycloak* 46

Figura 16 *Proceso de login con keycloak y prueba de vida* 47

Figura 17 *Ejemplo de modelo de detección de fraude* 54

Figura 18 *Protocolos Http vs WebSockets* 55

Figura 19 *Arquitectura modular* 56

Figura 20 *Proceso del módulo del banco de preguntas* 58

Figura 21 *Extensión de funcionalidad del flujo de login web en keycloak* 59

Figura 22 *Ejemplo de preguntas aleatorias generadas por el banco de preguntas* 62

Figura 23 *Evaluación de prueba de vida en modo debug* 63

Figura 24 *Pruebas realizadas* 64

Figura 25 *Ejemplo de prueba de vida exitoso integrado en login* 65

Resumen

Divide y vencerás es una frase muy conocida en el mundo del desarrollo de software y que sirve de norte para afrontar problemas muy complejos, sin embargo, también se puede usar esa frase a la inversa, la unión de pequeños desarrollos aislados que por sí mismos no representan más que la ejecución de una tarea sencilla, y que en conjunto pueden solventar problemas muy complejos como es el de realizar una verificación para determinar si el usuario que está interactuando con el sistema es una persona viva, eso es de lo que trata el presente proyecto de investigación ya que se diseñó un sistema de prueba de vida para login biométrico en web usando modelos de machine learning, para conseguirlo se utilizó de guía el método científico experimental con el fin de que el resultado de la búsqueda de diferentes modelos de inteligencia artificial durante cada iteración filtre modelos que se ajusten a la solución propuesta y descarte otros modelos que no aportaban al objetivo, se implementó el desarrollo en un ambiente contenerizado mediante Docker, la integración con el proveedor de identidades keycloak fue correcta y las pruebas sobre el sistema así como su integración en el flujo de login web de las aplicaciones segurizadas fueron satisfactorias.

Palabras clave: prueba de vida, inteligencia artificial, reconocimiento facial

Abstract

Divide and conquer is a well-known phrase in the world of software development and it serves as a guideline for tackling very complex problems. However, that phrase can also be used in reverse, the union of small isolated developments that by themselves do not they represent more than the execution of a simple task, and that together they can solve very complex problems such as carrying out a verification to determine if the user who is interacting with the system is a living person, that is what the present is about research project since a proof of life system was designed for biometric login on the web using machine learning models, to achieve this the experimental scientific method was used as a guide so that the result of the search of different artificial intelligence models during each iteration filter models that fit the proposed solution and discard other models that did not contribute to the objective, the development was implemented roll in a containerized environment using Docker, the integration with the keycloak identity provider was correct and the tests on the system as well as its integration in the web login flow of the secured applications were satisfactory.

Keywords: proof of life, artificial intelligence, facial recognition

Capítulo I

En todo tipo de desarrollo de software es fundamental entender al cliente y sus necesidades, es por esto que este capítulo trata acerca de la problemática existente en este entorno, permitiendo establecer lineamientos que ayuden como guía durante el proceso del desarrollo.

El avance informático hoy en día es abrumante y vertiginosamente veloz, por lo cual, estar a la vanguardia es fundamental, este capítulo trata de acercar al lector conceptos básicos que intervinieron en el desarrollo de este proyecto “sistema de prueba de vida para login biométrico usando modelos de machine learning”, tanto como componentes, aplicativos y herramientas con las que se trabajó durante todo el proceso, todo esto mediante estudios de literatura, gráficas y tablas explicando de la manera más adecuada su función y comportamiento esperado.

Introducción

Antecedentes

Kruger Corporation es una empresa de emprendimiento tecnológico que fue fundada por Ernesto Kruger en el año de 1993, durante toda su trayectoria han realizado diferentes proyectos de grande, mediana y pequeña magnitud, uno de sus principales clientes es la cadena de supermercados más grande del Ecuador “Corporación Favorita”, para la que se han desarrollado múltiples soluciones para diversas problemáticas surgidas en el transcurso del tiempo.

La cultura de Kruger Corporation se basa en una serie de valores tales como la alegría, el coraje, la empatía, el trabajo colaborativo, la agilidad, humildad, la capacidad crítica; Su misión es la innovación para el éxito de sus clientes en Iberoamérica y tiene como visión ser una corporación EXO con presencia

global. Kruger Corporation actualmente tiene presencia en 12 países los cuales son Panamá, Guatemala, Nicaragua, El Salvador, Costa Rica, Ecuador, Estados Unidos, Perú, Bolivia, Chile, Colombia y España.

Corporación favorita es una empresa ecuatoriana que cree e invierte dentro y fuera del país; Desarrollan áreas comerciales, industriales e inmobiliaria con presencia en Ecuador y 6 países de la región, según su página web [https://www.corporacionfavorita.com] posee en sus indicadores más de 20.000 (veinte mil) colaboradores, más de 11.000 (once mil) proveedores, 3.000.000 (tres millones) de clientes, más de 18.000 (diez y ocho mil) accionistas y generan más de 276.000 (doscientos setenta y seis mil) empleos indirectos, es una empresa cuya visión se basa en ser la mejor empresa de América, su misión es mejorar la calidad de vida ofreciendo los mejores productos, servicios y experiencias de forma eficiente sostenible y responsable, se fundamenta en los valores de: confianza, liderazgo, contribución, integridad, armonía y felicidad.

Problemática

Corporación Favorita solicitó un mecanismo de autenticación biométrico para evitar fraudes y que pueda asegurar la identidad de los clientes, para lo cual se requirió desarrollar un login biométrico que permita obtener una prueba de vida del usuario que intenta acceder al o los sistemas segurizados.

Objetivos

Objetivo General

Diseñar un sistema de prueba de vida para login biométrico en web usando modelos de machine learning.

Objetivos Específicos

i. Investigar modelos de machine learning que permitan el reconocimiento facial.

ii. Investigar sobre el uso del paradigma de servicios web para la codificación del sistema web

iii. Diseñar una solución que permita la integración de los servicios de prueba de vida para el proveedor de identidades y accesos keycloak.

iv. Realizar pruebas y evaluar resultados.

Justificación

En este proyecto se desarrolló un sistema de servicios web que permite obtener una prueba de vida del usuario que está realizando el login biométrico, demostrando que es una persona y no un algún tipo de Spoofing, esto se consiguió basándose en biometría facial con interacciones aleatorias que debe realizar el usuario.

Alcance

En el presente proyecto de investigación, se planteó como alcance el desarrollo de una API que contenga la lógica de sistema de prueba de vida para login biométrico y una página web para poder realizar las pruebas del funcionamiento correcto de la misma.

Marco teórico

Antes de abordar la problemática del desarrollo de un mecanismo de autenticación biométrico para evitar fraudes y que pueda asegurar la identidad de los clientes, se tiene que mencionar diferentes conceptos de las herramientas que fueron utilizadas en el proceso de la solución propuesta en este documento.

Docker

Docker es una tecnología que permite contenerizar ambientes controlados para qué el desarrollo sea eficiente y predecible, eliminando las tareas de configuración repetitivas y se usa durante todo el ciclo de vida del proyecto para un desarrollo de aplicación rápido, fácil y portátil, tanto en escritorio como en la nube, las imágenes Docker permiten a los desarrolladores ejecutar aplicaciones en diferentes entornos de manera consistente ahorrando los engorrosos problemas de configuraciones,de esta forma se evita el típico “En mi maquina si funcionaba”. (Docker, s.f.)

Docker también ofrece un servicio de alojamiento de imágenes [https://hub.docker.com/] para todos sus usuarios de manera gratuita, esto es conveniente ya que se puede encontrar aplicaciones oficiales que sirven para desarrollar aplicaciones rápidamente, por ejemplo, se puede encontrar imágenes de diferentes bases de datos como MySQL, solo se necesita descargar la versión que se requiere en el entorno de desarrollo, pruebas o producción y de esta manera la configuración de un ambiente de base de datos esta lista para ser usada.

Python

"Python es un lenguaje de programación que permite trabajar rápidamente e integrar sistemas de manera más efectiva." En el campo de la Inteligencia Artificial es muy común el uso de este lenguaje para el desarrollo de soluciones, por la facilidad y gran cantidad de información que se puede encontrar en internet es el lenguaje que se utilizó en el desarrollo del API de este proyecto. (Python, 2021),

HTML, CSS, JS

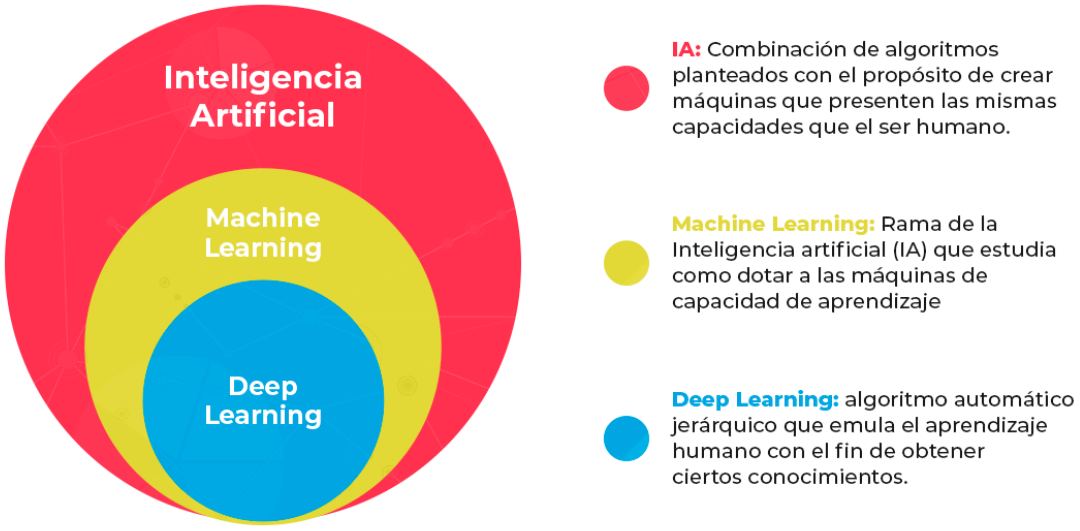
La gran mayoría de sistemas necesita la interacción del usuario, y es por esto que se utilizó los lenguajes HTML, CSS y JS, para el desarrollo del front-end de este proyecto. "HTML es el lenguaje de marcado estándar para páginas web." (w3schools, 2021); "CSS es el lenguaje que usamos para diseñar un documento HTML. CSS describe cómo se deben mostrar los elementos HTML." (w3schools, 2021); "JavaScript es el lenguaje de programación más popular del mundo. JavaScript es el lenguaje de programación de la Web." (w3schools, 2021);

Inteligencia artificial

En este documento se usó diferentes modelos de inteligencia artificial, en la Figura 1 se muestra un mapa conceptual para tener claro exactamente a qué se refiere cuando se habla de inteligencia artificial, machine learning, redes neuronales, Big Data o Deep learning, muchos conceptos que normalmente se solapan o se interpretan de diferente manera y que al final acaban siendo utilizados con mucha confusión.

Figura 1

Mapa de la Inteligencia Artificial



Nota. Tomado de https://www.masterdatascienceucm.com/que-es-machine-learning/

En realidad, intentar definir lo que es la inteligencia artificial es una tarea muy complicada, sobre todo porque es un concepto que depende del propio significado de inteligencia, que hoy en día sigue teniendo múltiples interpretaciones, es por esto que cuando se intenta precisar lo que es la inteligencia artificial, encontramos también a muchos autores que la definen a su manera.

Según (Amador Hidalgo, 1996), en su libro "Inteligencia Artificial y Sistemas Expertos" menciona que *"La Inteligencia Artificial es el estudio de la inteligencia como proceso. Este último término, proceso, no implica siempre obligatoriamente operaciones numéricas, sino que indica los procedimientos efectivos por medio de los cuales se pueden generar comportamientos inteligentes"*, por otro lado, según (Boden, 1984) en su libro "Inteligencia Artificial y Hombre Natural" explica que *"La Inteligencia Artificial no es el estudio de las computadoras. Las computadoras son máquinas metálicas de interés intrínseco*

para la Ingeniería Electrónica (...). Por inteligencia Artificial, en consecuencia, se entiende el uso de programas de computadora y de técnicas de programación para proyectar luz sobre los principios de la inteligencia en general y de la inteligencia humana en particular (...). De ello se sigue que no se hace ninguna distinción básica de principio entre la Inteligencia Artificial· y la simulación por computadora. Desde luego hay una diferencia de acento entre las investigadoras (sic.) Que intentan hacer una máquina que haga algo, independientemente de cuán humano sea, y las que pretenden escribir un programa que sea equivalente funcionalmente a una teoría psicológica", y por tomar un concepto adicional tenemos según (Rouhiainen, 2018) quien dice en su libro "Inteligencia artificial – 101 cosas que debes saber hoy sobre nuestro futuro" que Inteligencia Artificial es *"la habilidad de los ordenadores para hacer actividades que normalmente requieren inteligencia humana"*, pero, si se toman todas estas definiciones y se extrae una idea común, se tiene que la inteligencia artificial es una disciplina del campo de la informática que busca la creación de máquinas que puedan imitar comportamientos inteligentes, estos comportamientos pueden ser muy diversos; desde conducir a analizar patrones, reconocer voces o ganar en juegos.

Son muchas las formas en las que una máquina puede simular un comportamiento inteligente y cada vez se tiene más ejemplos de cómo en ciertas áreas logran alcanzar un rendimiento mayor al humano, sin embargo, ¿eso las convierte en más capaces que un humano? No exactamente, si se toma a cualquiera de estas Inteligencias artificiales que sobresalen en un dominio muy específico y se intenta realizar otra tarea, el resultado que se obtiene es desastroso, esta capacidad de poder realizar múltiples tareas es la que permite al ser humano, por ejemplo, realizar al mismo tiempo acciones como pensar, ver, andar y hablar, la característica de ejecutar diversas tareas es muy codiciada y se sigue investigando en los departamentos de inteligencia artificial. (Santana Vega)

Tipos de Inteligencia artificial.

La Tabla 1 presenta a una primera clasificación de los tipos de Inteligencia artificial, por un lado las débiles y por otro las fuertes; "*se dice que una inteligencia artificial es débil, cuando son aquellos sistemas que únicamente pueden cumplir con un conjunto muy limitado de tareas, por ejemplo, por mucho que haya entrenado a un robot a caminar, al intentar hacer algo diferente como patear una pelota puede que no se obtenga el resultado esperado"* (Santana Vega) , por el contrario, "*las Inteligencias artificiales fuertes hacen referencia a aquellos sistemas que son capaces de aplicarse a una gran variedad de problemas y dominios diferentes"* (Santana Vega), sin embargo, a día de hoy, todas las Inteligencias artificiales todavía se clasifican en el primer grupo, por mucho que las películas de Hollywood hayan mostrado ejemplos de Inteligencias artificiales fuertes hace ya muchos años.

Tabla 1

Comparación entre Inteligencias artificiales Débiles y Fuertes

IA Débil	IA Fuerte
La IA débil es simplemente la opinión de que las computadoras pueden modelar y utilizar el comportamiento inteligente para resolver problemas complejos.	La IA fuerte se refiere a una máquina hipotética que exhibe habilidades cognitivas humanas.
La IA débil se refiere a los sistemas que están programados para resolver una amplia gama de problemas pero que operan dentro de una gama predefinida de funciones.	La IA fuerte se refiere a máquinas con mente propia y que pueden pensar y realizar tareas complejas por sí mismas.
Las máquinas débiles impulsadas por IA no tienen mente propia.	Las máquinas potentes impulsadas por IA pueden exhibir fuertes habilidades cognitivas humanas.
Alexa y Siri son los mejores ejemplos de programas de inteligencia artificial débiles.	La IA fuerte es un concepto hipotético que aún no existe en su forma real.

Nota. Tomado de https://forum.huawei.com/enterprise/es/%C2%bfalg%C3%ban-ejemplo-de-ia-fuerte-en-la-actualidad/thread/741535-100757

Comportamientos inteligentes

Si se toma la definición mencionada anteriormente de Inteligencia Artificial, es importante remarcar lo de "***imitar comportamientos inteligentes"*** porque es la clave para entender el resto de conceptos que se van a mencionar; Imitar, no significa que dicho comportamiento sea en esencia un

comportamiento cognitivo, es decir, se puede programar de manera clásica los movimientos de un brazo robótico para que siempre realice un mismo movimiento, eso en principio no parece muy inteligente, ya que la lógica del movimiento del brazo ha sido programada, pero esto encaja dentro de la definición que se ha dado, porque en apariencia la máquina realiza un comportamiento inteligente, visto así, dentro del campo de la inteligencia artificial se puede encontrar diferentes subcategorías que responden a diferentes comportamientos inteligentes. (Santana Vega).

Los ejemplos de la Tabla 2 conforman campos de estudios propios dentro del mundo de la inteligencia artificial, sin embargo, si hay una capacidad que de verdad define como agentes inteligentes es la capacidad de aprender es decir el machine learning,

Tabla 2

Ejemplos de Capacidades de las Inteligencias artificiales y sus campos de estudio

Capacidad	Campo / Categoría
Moverse y adaptarse al entorno	Robótica
Entender lenguaje natural, cambios de voz a texto o texto a voz	Procesamiento de Lenguaje Natural
Analizar patrones y características en imágenes	Visión por Ordenador

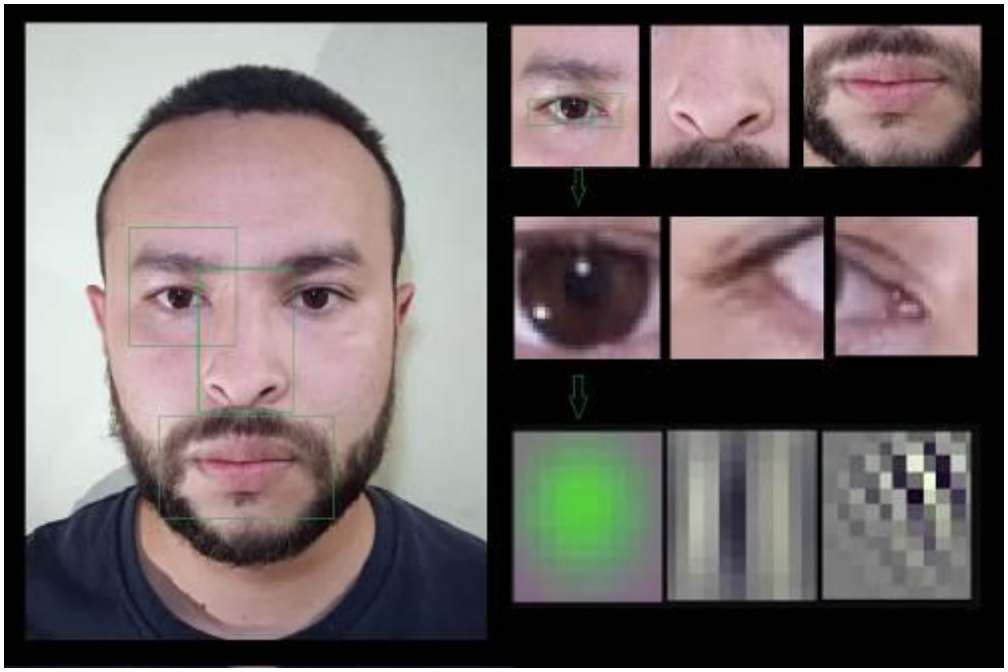
Machine learning

El machine learning o aprendizaje automático es “La rama de la inteligencia artificial que estudia cómo dotar a las máquinas de capacidad de aprendizaje” (Arthur, 1959), entendido este como, la generalización del conocimiento a partir de un conjunto de experiencias, este aprendizaje puede dividirse en tres grupos diferentes: aprendizaje supervisado, no supervisado y reforzado.

Por tanto, se tiene claro que el machine learning es una disciplina dentro del campo de la inteligencia artificial, pero no es una disciplina cualquiera, es un componente nuclear que de hecho se relaciona y conecta con el resto de categorías, porque las otras capacidades pueden ser imitadas, ya sea porque alguien las haya programado o mucho más interesante porque el propio sistema haya aprendido a realizarlas; una cosa es programar una máquina para que pueda moverse y otra muy diferente es programarla para que aprenda a moverse, igualmente, no es lo mismo programar qué elementos conforman una cara (Figura 2), que aprender automáticamente qué es una cara.

Figura 2

Elementos que conforman una cara



Este cambio de paradigma es lo que hace interesante al machine learning, y por ello, es muy común confundir la parte por el todo, es decir, errar en que la inteligencia artificial y el machine learning es la misma cosa.

Técnicas de machine learning

Dentro del machine learning se encuentra un nuevo mundo donde existen diferentes técnicas que sirven para cubrir diferentes tipos de aplicaciones, por ejemplo, existen técnicas como los árboles de decisión, modelos de regresión, modelos de clasificación, técnicas de clusterización, y muchas otras más (Figura 4), sin embargo, si una de estas técnicas ha dado fama al campo del machine learning

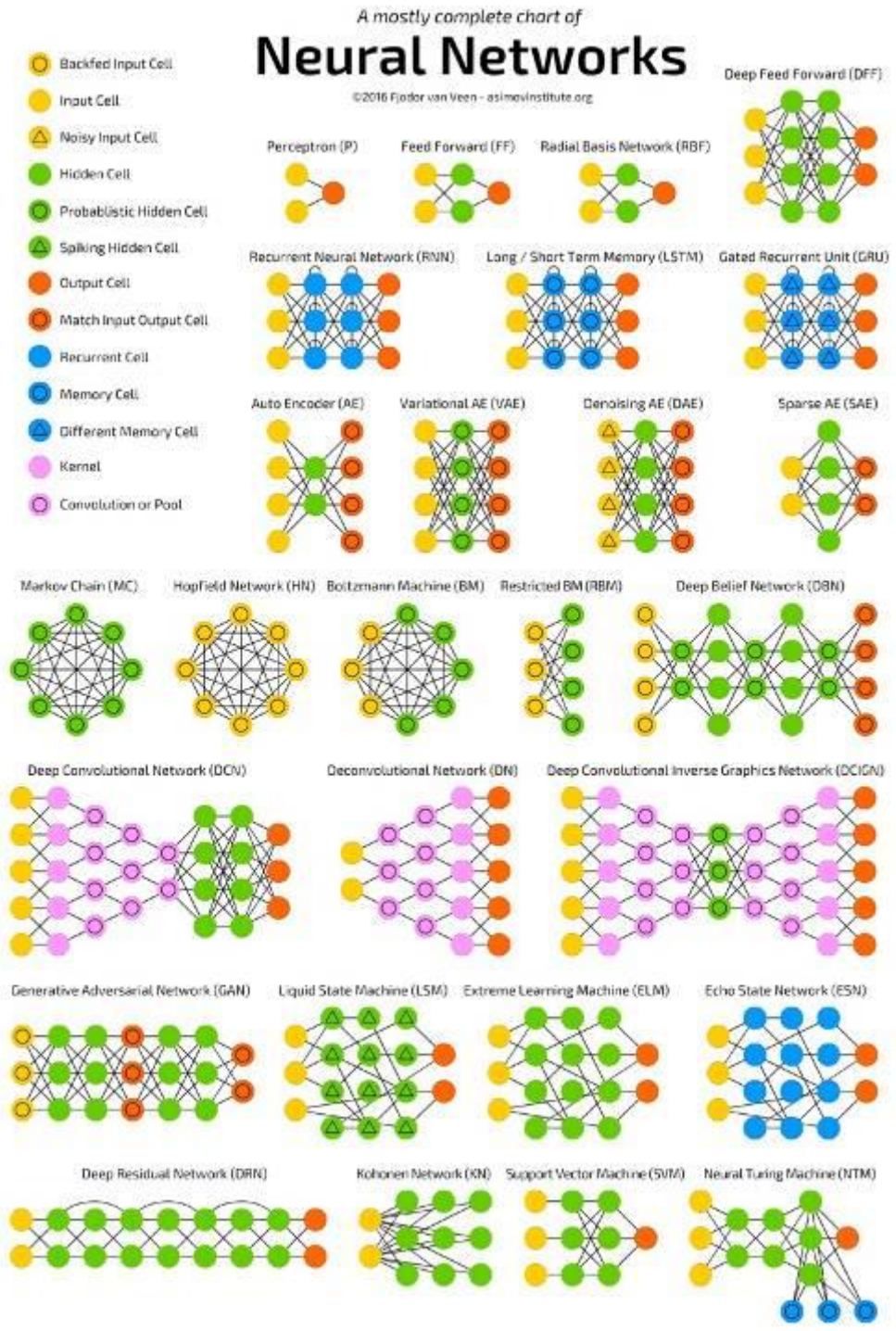
durante la última década, son las redes neuronales; lo interesante de las redes neuronales, es que son capaces de aprender de forma jerarquizada, es decir, la información se aprende por niveles, donde las primeras capas aprenden conceptos muy concretos como por ejemplo: que es un tornillo, un espejo, una rueda, y en las capas posteriores se usa la información aprendida previamente para conceptualizar información más abstracta como por ejemplo: que es un coche, un camión, una moto; esto hace que a medida que se añade más capas la información que se aprende es cada vez más abstracta e interesante (Figura 3). (Torrubia)

Figura 3

Ejemplo de conceptualización de las redes neuronales en diferentes capas

Figura 4

Diagrama de las redes neuronales



Nota. Tomado de https://decodigo.com/2018/04/un-diagrama-casi-completo-de-las-redes-neuronales.html

Deep learning

Pero… ¿Y cuántas capas se puede poner? Realmente no hay límite, y la tendencia es que cada vez estos algoritmos añadan más y más capas convirtiéndose en algoritmos cada vez más complejos, este incremento en el número de capas y en la complejidad es lo que hace que estos algoritmos sean conocidos como algoritmos de Deep learning.

¿En realidad se necesitan estas técnicas tan complejas? La respuesta es que si, imagina que estas técnicas se entrenan y aprenden a partir de los datos, y actualmente la humanidad está inmersa en la era de la información, con la llegada de la digitalización, el abaratamiento de los dispositivos de almacenamiento y un cambio de mentalidad a la hora de apreciar el valor de los datos, se ha entrado en una tendencia de acumular más y más datos, algo que se ha denominado Big data. (Santana Vega)

Redes neuronales convolucionales

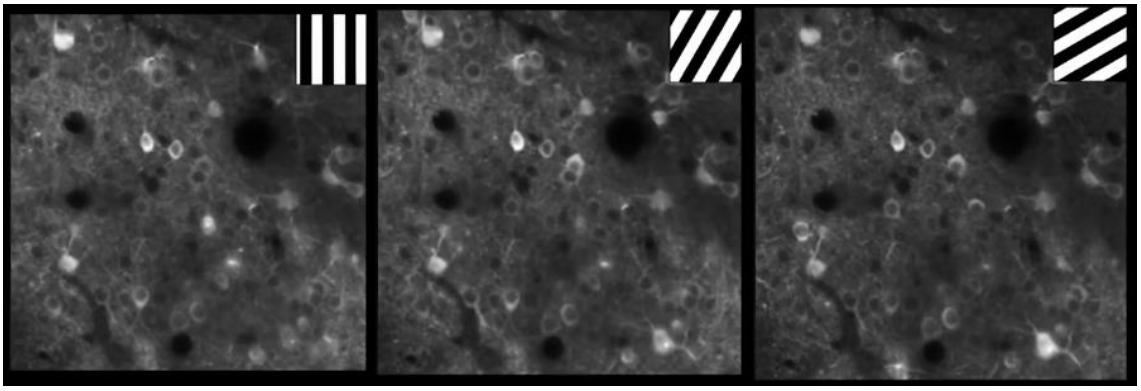
Estas redes están especializadas en trabajar con imágenes, la importancia de estas redes viene de su capacidad de poder descifrar los patrones más complejos en enormes data sets de imágenes dotando de “ojos” a las máquinas, que tanto pueden observar rostros de personas, radiografías de pacientes, o los peatones que se cruzan ante un coche autónomo, se ha conseguido que las máquinas puedan percibir el mundo que les rodea. (Torrubia)

Se debe entender bien los principios básicos que hay detrás del proceso de visión humana para poder comprender la visión artificial, si una persona revisa la Figura 2 se puede decir ¿qué es lo que está viendo?, la respuesta de seguro fue que en el lado izquierdo hay una cara, esto es porque seguramente

ha escaneado la imagen y ha detectado la presencia de algunos elementos que por el aprendizaje adquirido sabe que conforman a un rostro, *aquí hay ojos, aquí hay una boca, aquí hay una nariz…*; Pero ¿Por qué una persona sabe que hay un ojo? Bueno, porque ha detectado una serie de elementos que conforman normalmente a un ojo, *una pupila negra, líneas que son pestañas, superficies blancas;* y todo esto también lo ha sabido reconocer, porque es capaz de detectar *patrones circulares, cambios de contrastes, texturas* y así sucesivamente, al final si se reproducen los pasos que realiza el córtex visual, se encuentra un procesamiento en cascada donde primero se identifican aquellos elementos básicos y generales, y en posteriores capas esto se combina para generar patrones cada vez más complejos (Figura 10).

Figura 5

Estimulación de neuronas con patrones

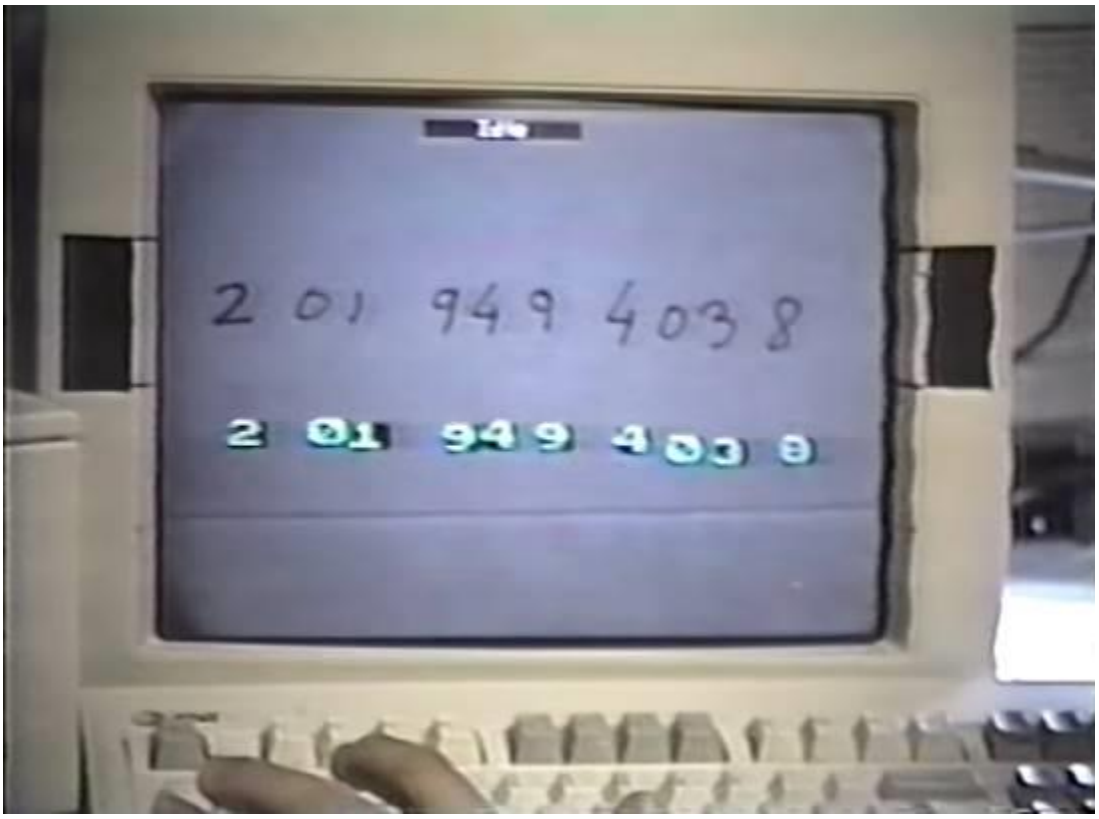


Nota. Tomado de Una selva de sinapsis**.** En la Ilustración se muestra la activación ante la estimulación de diferentes neuronas cerebrales con diversos patrones

Este concepto fue la inspiración para investigadores como (Le Cun, y otros, s.f.), quienes en el paper “Handwritten digit recognition with a back-propagation network” introdujeron el primer diseño de una red neuronal convolucional para la detección de números escritos en cheques bancarios (Figura 6).

Figura 6

Evaluación del diseño de una CCN para la detección de números escritos en cheques bancarios

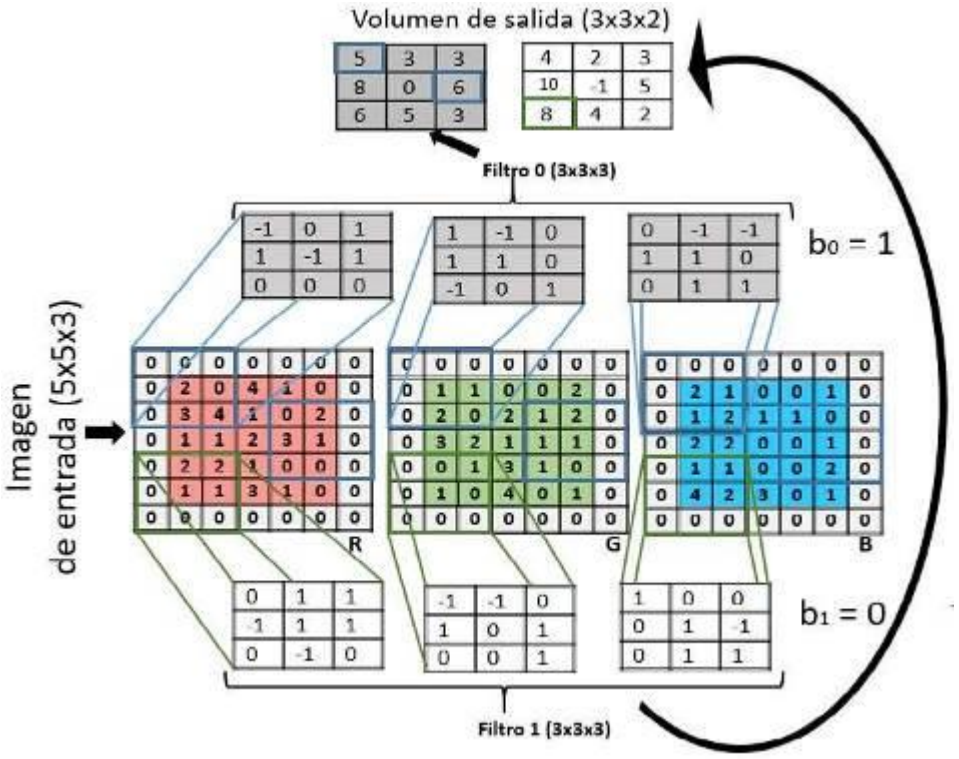


Nota. Tomado de Yann LeCun Convolutional Network Demo from 1993 [https://youtu.be/FwFduRA_L6Q]

Pero, ¿Qué es una red neuronal convolucional?, Es un tipo de red neuronal cuyo diseño ha sido pensado para sacar partido a algo muy evidente que se encuentra en una imagen su estructura espacial (en sus ejes X & Y), es decir, es un tipo de red neuronal que se caracteriza por aplicar un tipo de capa donde se realiza una operación matemática conocida como convolución (Figura 7). (Torrubia)

Figura 7

Ejemplo de convolución con dos filtros de 3x3 en una imagen RGB de 5x5

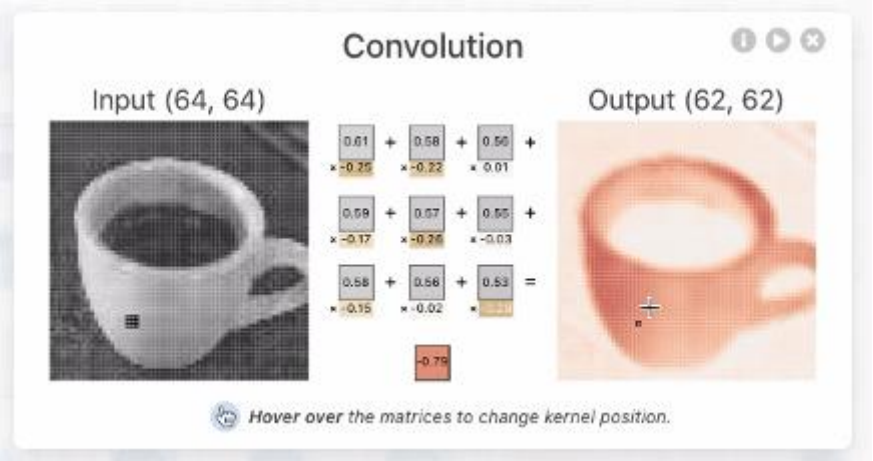


Nota. Tomado de https://www.researchgate.net/figure/Figura-210-Ejemplo-de-convolucion-con-dos-filtros-de-3x3-en-una-imagen-RGB-de-5x5_fig3_323460108

Una convolución aplicada sobre una imagen, no es más que una operación que, jugando con los valores de los píxeles, es capaz de producir una nueva imagen, concretamente cada pixel nuevo que vayamos a generar se calculará colocando una matriz de números llamados filtros o kernel sobre la imagen original, y donde se multiplica y se suman los valores de cada pixel vecino para obtener el nuevo valor, esto se realiza desplazando el filtro y realizando esta operación por toda la imagen; Aquí dependerá de cómo se configuran los parámetros de nuestro filtro para obtener un resultado u otro (Figura 8).

Figura 8

El kernel que se aplica para producir el resultado intermedio más alto para el mapa de activación



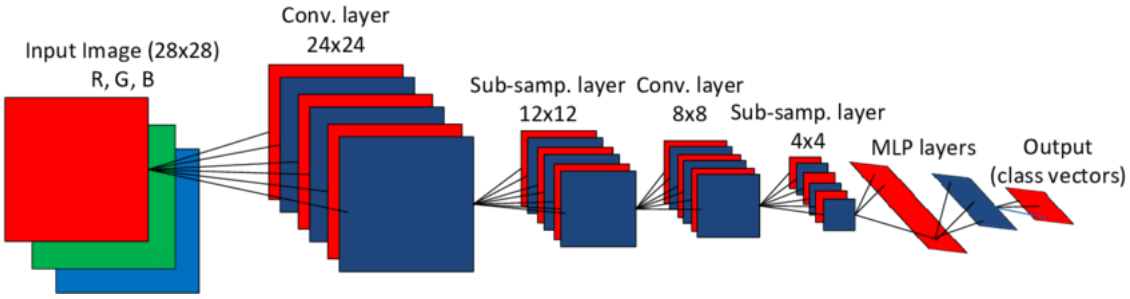
Nota. Tomado de Captura de pantalla de https://poloclub.github.io/cnn-explainer/

Lo que hay que entender es que esta operación de convolución sobre una imagen, puede detectar cosas diferentes según cuáles sean los valores del filtro que se defina, o mejor dicho los valores del filtro que la red irá aprendiendo poco a poco en su entrenamiento, para poder hacer mejor su tarea.

Aprender estos filtros para detectar patrones, es el principal trabajo de la red neuronal convolucional, a cada una de las imágenes generadas se le conoce como un mapa de características, ya que actúa como un mapa donde se nos indica en qué parte de la imagen se ha detectado la característica buscada por dicho filtro, cada pixel blanco, será una activación que nos indique que el elemento buscado estaba ahí, por tanto, a una imagen se aplica una serie de convoluciones y este genera un conjunto de mapas de características, el potencial de este tipo de redes se encuentra en que esta operación se va a realizar secuencialmente donde el output de una de las capas se va a convertir en el input de la siguiente.

Figura 9

Ejemplo de una red convolucional estándar



Nota. Tomado de https://www.researchgate.net/figure/A-standard-2D-CNN-10_fig2_313676923

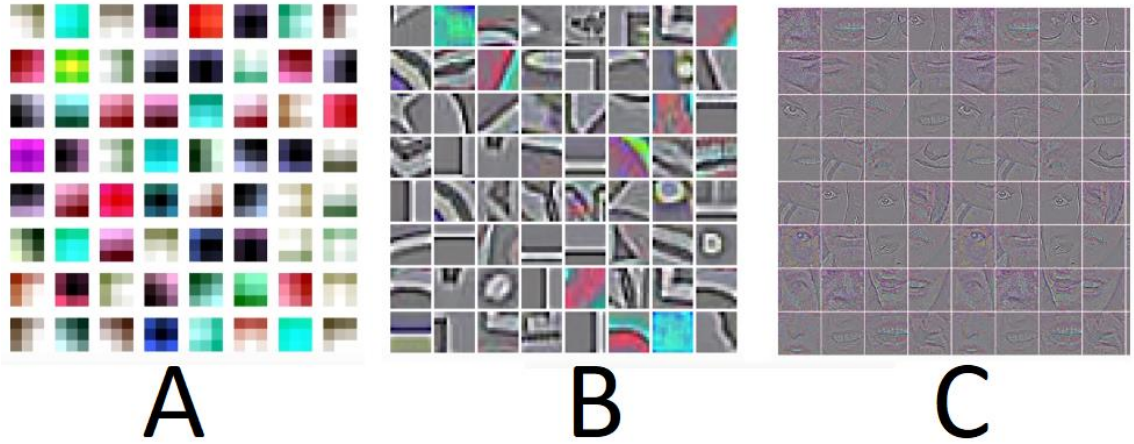
En la Figura 9, el input es una imagen normal a color con los tres canales RGB, esto se podría interpretar como que en realidad se tiene tres mapas de características diferentes donde se han detectado elementos en rojo, en verde y en azul, existe tres mapas de características donde se realiza la operación de convolución con seis filtros, se va a detectar seis cosas diferentes, que darán como resultado 6 mapas de características, seis imágenes que ahora pasarán a ser el input de la siguiente capa de convolución.

Se puede utilizar filtros de tamaño 3x3, 5x5 o 7x7 píxeles, para ir escaneando poco a poco la imagen buscando patrones, pero ¿esto es suficiente? ¿es posible que un filtro tan pequeño pueda detectar patrones tan complejos como por ejemplo un ojo o una llanta? ¿es posible que un filtro detecte todo esto?, lo que sucede es que, la operación de convolución cada vez se va a ir haciendo más potente, porque donde antes se tenía una región de nueve píxeles nuestro filtro de 3x3 lo ha convertido en un único píxel de información y, por tanto, si se vuelve a aplicar ahora una convolución sobre estos mapas de características resultantes en realidad se está accediendo cada vez a más información espacial de la imagen original.

Las convoluciones no dejan de ser operaciones que pueden detectar cambios de contraste, texturas, superficies planas, pero si se van acumulando a través de las capas, se pueden ir descubriendo patrones cada vez más complejos Figura 10.

Figura 10

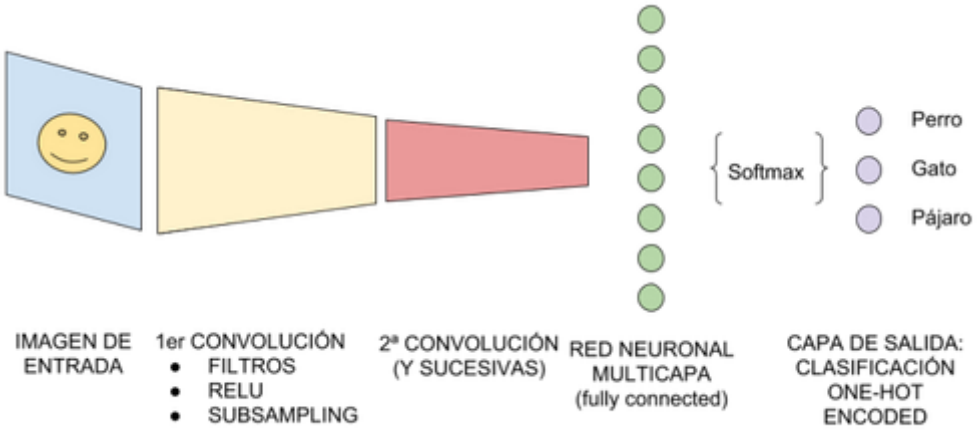
Ejemplo de filtros que detectan patrones complejos a medida que se realizan las convoluciones en cada capa



¿Y dónde acaba todo esto?, Bueno, cuando la imagen ya pasa por todo el embudo convolucional, llega a un punto donde se ha detectado todos los patrones necesarios y se tiene muchos mapas de características, todo esto son los inputs independientes dentro de una red neuronal multicapa, esta red termina aprendiendo que es lo que hay en esa imagen (Figura 11).

Figura 11

Arquitectura de una Red neuronal Convolucional



Nota. Tomado de https://www.juanbarrios.com/redes-neurales-convolucionales/

Modelos de inteligencia artificial

Un modelo, es una construcción simplificada de una realidad más compleja; el humano vive en un universo en constante evolución, complejo, caótico y lleno de ruido y, sin embargo, la inteligencia humana consigue dar sentido a todo este caos, en una búsqueda por la elegancia y la simetría que se esconde entre los patrones que identifica en la realidad. (Santana Vega)

El desarrollo de la especie humana se ha debido principalmente a esta capacidad de saber detectar patrones y poder utilizarlos a favor, la ciencia ha permitido explotar la capacidad de observar el mundo de manera simplificada convirtiendo todo este ruido en conocimiento, es decir, reconstruyendo la realidad a través de modelos. (Santana Vega)

Mediante esta reconstrucción el hombre es capaz de entender mejor dicha realidad y poder utilizarla a su favor, convive diariamente con diferentes tipos de modelos, por ejemplo, un mapa urbano sería un tipo de modelo ya que permite representar de manera simplificada en un plano bidimensional el mundo tridimensional en el que vive, eliminando detalles innecesarios como texturas o artefactos del entorno. (Santana Vega)

Un modelo busca el equilibrio entre aproximarse a representar correctamente la realidad y ser simple para poder utilizarlo, por ejemplo si se quiere modelar el comportamiento natural de las aves, primero se debe recopilar diferentes evidencias y tras la observación, se puede enunciar un primer modelo de su comportamiento, [*las aves pueden volar*]; si se sigue recopilando evidencias se descubre que este modelo es muy simple, ya que hay aves que todavía no han aprendido a volar y otras que estando heridas tampoco pueden, por tanto, se actualiza el modelo y se dice que, [*si una ave es adulta y no está herida puede volar*], parece ahora así que el modelo se ajusta más a la realidad, pero de repente aparecen pingüinos y, se puede seguir ajustando el modelo y las diferentes variaciones de la realidad que se está estudiando, pero al final, se termina teniendo un modelo muy complejo con todas las excepciones de por qué un ave vuela o no; una alternativa a esto es hacer uso de la probabilidad, para poder decir matemáticamente que [*la mayoría de aves pueden volar*].

La probabilidad es la herramienta perfecta para resumir la incertidumbre sobre un tema, ya sea por falta de conocimiento o por pereza, ¿que es mejor decir? que un plato se romperá dependiendo de la fuerza inicial de lanzamiento, del material del plato, o de si alguien evita cogerlo durante la caída, la elasticidad de la superficie donde cae, el punto de impacto, etcétera; o decir, que un plato se rompe en el 93% de las ocasiones, utilizar la probabilidad para construir modelos da como resultado los modelos probabilísticos. (Santana Vega)

Estos modelos comprimen en base a probabilidades mucha de la variabilidad de la realidad siendo más sencillo de gestionar la información que se recibe del entorno, el cerebro aplica esquemas similares a estos modelos probabilísticos y gracias a ellos, se tiene capacidades como la de conceptualizar, predecir, generalizar, razonar o aprender, por esto mismo, descubrir cuáles son estos modelos es uno de los objetivos básicos del campo del machine learning. (Santana Vega)

Detección de rostros

La detección de rostros fue una parte fundamental en la solución de la problemática de este proyecto de investigación "sistema de prueba de vida para login biométrico usando modelos de machine learning", se encontró una comparativa sobre los diferentes modelos existentes para la detección de rostros. En esta se mencionan parámetros que se deben considerar al momento de seleccionar el modelo de Inteligencia artificial a usar. (Solano, s.f.)

Según (Agarval, 2022) quien compara cuatro modelos de diferentes arquitecturas que realizan la detección de rostros, las principales características que evaluó fueron [ángulos de la cara, oclusión del rostro, condiciones de iluminación, cuadros por segundo]. Se realizaron pruebas con los modelos HAAR, DLIB, MTCNN y DNN. Si bien, en esta investigación el modelo recomendado fue el DNN, en este proyecto se hizo uso del modelo HAAR, debido a que no solamente se requiere detectar un rostro sino también los Landmarks de para poder utilizarlos en los diferentes modelos de inteligencia artificial involucrados en la solución.

El modelo HAAR Cascade permite encontrar en una imagen el rostro de una o varias personas mientras que ignora el fondo de la imagen u otros objetos que estén presentes dentro de ella, detectar

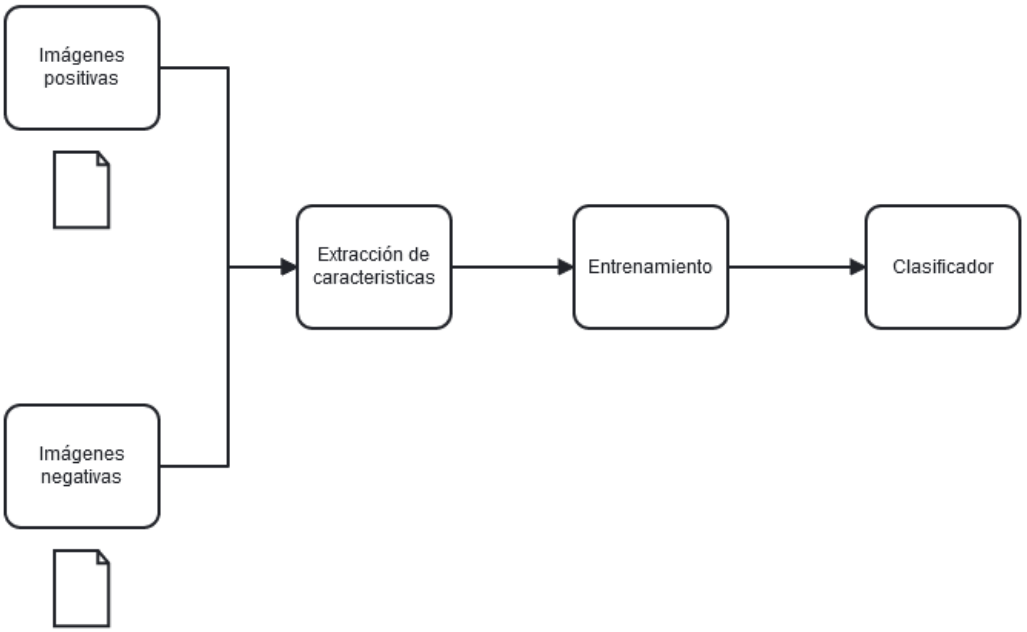
un rostro en una imagen sin duda no es una tarea fácil para el computador por ello se necesita que éste ”aprenda”, mediante técnicas de machine learning, se necesita una gran cantidad de imágenes para entrenar a un clasificador para que éste pueda discernir entre la presencia de un objeto y la ausencia presencia del mismo. (Solano, s.f.)

HAAR Cascade fue publicado por primera vez por Paul Viola y Michael Jones (Viola & Jones, 2001), proponen un algoritmo que es capaz de detectar objetos en imágenes, independientemente de su ubicación y escala en una imagen. Además, este algoritmo puede ejecutarse en tiempo real, lo que permite detectar objetos en transmisiones de video.

¿Cómo trabaja un detector de rostros?, Para realizar un detector de rostros se requieren imágenes positivas, es decir, imágenes con rostros e imágenes negativas que serían imágenes que no contengan rostros, estas imágenes son el input para el entrenamiento de un clasificador de imágenes donde extrae características de todas estas imágenes, finalmente se podrá obtener un clasificador que identifique la existencia o ausencia de un rostro en una imagen (Figura 12).

Figura 12

Pasos para el entrenamiento de un clasificador de imágenes



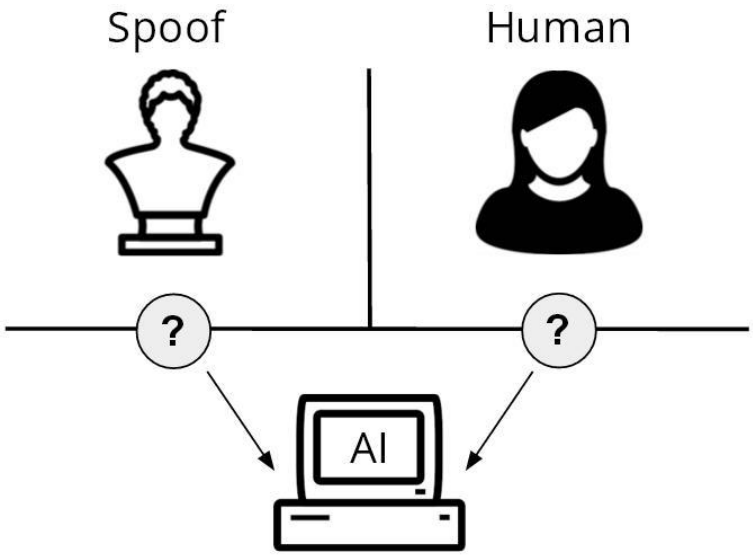
En este proyecto se utilizaron los clasificadores pre entrenados que ofrece OpenCV en su repositorio GitHub (OpenCV, 2022).

Prueba de vida

Una prueba de vida o detección de vida “es la capacidad de una computadora para determinar que está interactuando con un ser humano físicamente presente y no con un artefacto de parodia inanimado o video / datos inyectados.” (Tussy, Wojewidka, & Josh Rose, 2021), este concepto fue fundamental en la estructuración de los requerimientos del proyecto de investigación “sistema de prueba de vida para login biométrico usando modelos de machine learning”.

Figura 13

Liveness Detection es una IA que determina si una computadora está interactuando con un ser humano vivo



Nota. Tomado de https://liveness.com/.

Determinar si la interacción de un sistema es con una persona o con otro sistema que emula ser una persona es una tarea complicada, Tussy, Wojewidka, & Josh Rose mencionan que existen diferentes niveles de amenaza describiendo cinco niveles ellos denominan parodia, divididos en dos grupos, los artefactos y las derivaciones, es artefacto cuando un objeto no vivo exhibe rasgos humanos como se aprecia en la Tabla 3, por otro lado una derivación sucede cuando se manipulan los datos biométricos después de la captura o se omite la cámara por completo (Tabla 4).

Tabla 3

Tipos de artefactos utilizados en la suplantación de identidades

Tipo de artefacto	Descripción	Ejemplo
Nivel 1 (A)	Fotos digitales y en papel de alta resolución, videos de desafío / respuesta de alta definición y máscaras de papel. Cuidado: las pruebas de laboratorio de ibeta NO incluyen ataques de marionetas deepfake, pero Spoof Bounty de facetec SÍ incluye marionetas deepfake.	
Nivel 2 (B)	Muñecas realistas disponibles comercialmente y máscaras 3D de resina, látex y silicona usadas por humanos con un precio inferior a $ 300.	
Nivel 3 (C)	Máscaras 3D ultrarrealistas hechas a medida, cabezas de cera, etc., con un costo de creación de hasta $ 3,000.	

Nota. Tomado de https://liveness.com/.

Tabla 4

Tipos de derivación utilizados en la suplantación de identidades

Tipo de derivación	Descripción	Ejemplo
Nivel 4	Descifre y edite el contenido de un 3D facemap ™ para que contenga datos sintéticos no recopilados de la sesión, haga que el servidor procese y responda con Liveness Success.	
Nivel 5	Toma el control de la alimentación de la cámara e inyecta fotogramas de video capturados previamente o una marioneta falsa que da como resultado que facetec AI responda con "Liveness Success".	

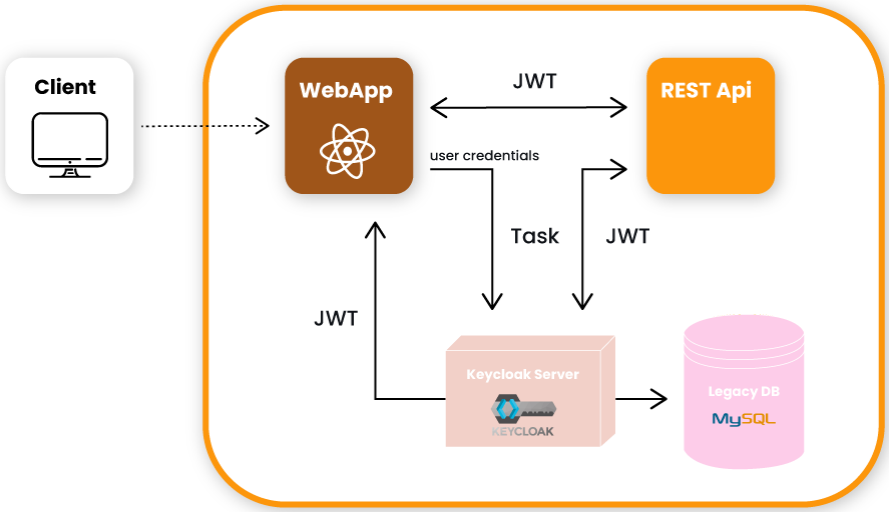
Nota. Tomado de https://liveness.com/.

Proveedor de identidades y accesos

Un proveedor de identidades y accesos es una aplicación y/o servicios que gestionan toda la lógica que se encuentra detrás de la autenticación y servicios seguros, hacen uso de estándares y protocolos para la fácil implementación. En el desarrollo de este proyecto de investigación se utilizó el proveedor de identidades “Keycloak”, en la Figura 14 se puede identificar el flujo general con el que trabaja este proveedor de identidades.

Figura 14

Flujo genérico de Keycloak

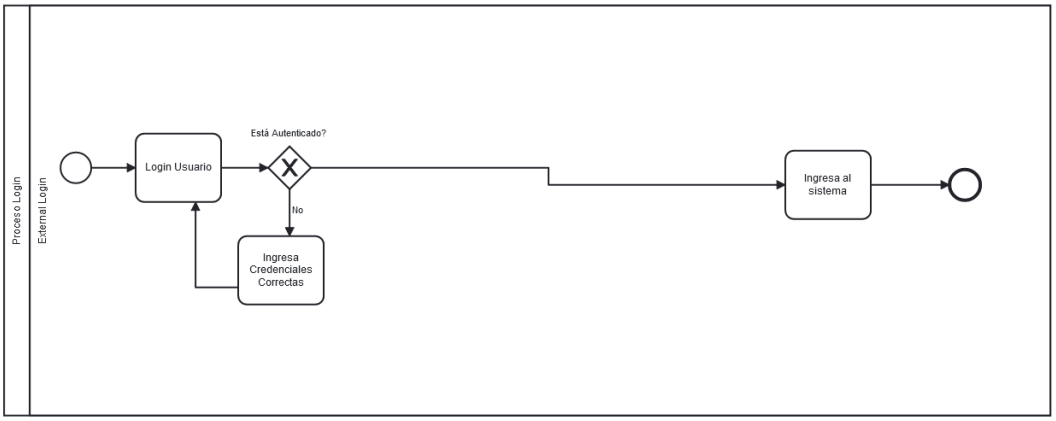


Nota. Tomado de https://medium.com/flux-it-thoughts/autenticaci%C3%B3n-enterprise-integrada-con-keycloak-parte-2-589070aea2f4

El flujo del cual se partió para el login de Corporación Favorita empieza con el envio del formulario donde se cargan usuario y contraseña, esos datos van al servidor de keycloak y este retorna los tokens que van a servir para la comunicación continua del sistema segurizado durante la interacción del usuario como se muestra en el flujo de la Figura 15.

Figura 15

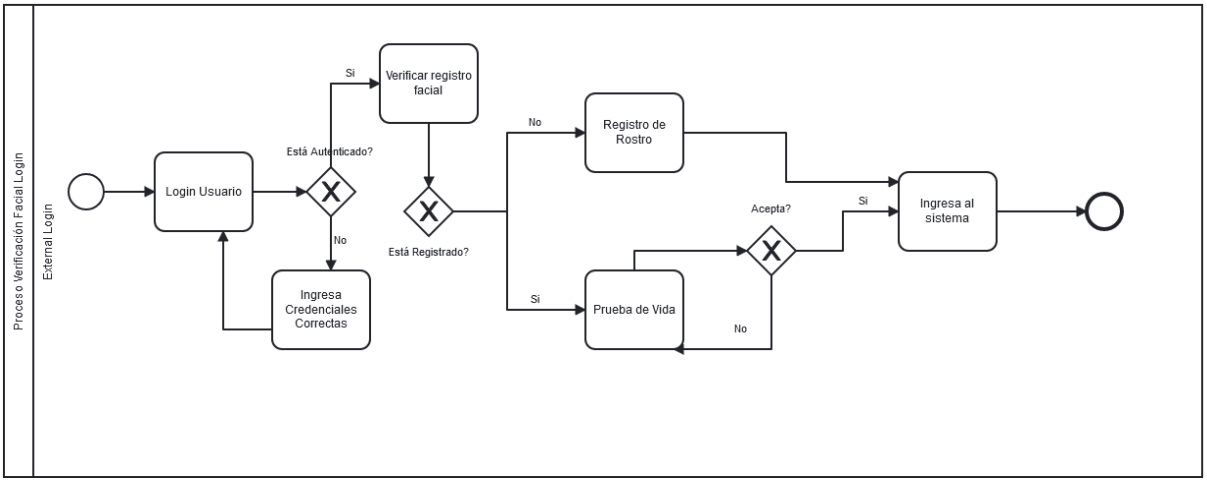
Proceso de login con keycloak



La propuesta en la solución de la problemática de este proyecto de investigación “sistema de prueba de vida para login biométrico usando modelos de machine learning”, fue integrar como segundo factor de autenticación la prueba de vida, es decir, el login de Corporación Favorita empieza con el envío del formulario donde se cargan usuario y contraseña, esos datos van al servidor de keycloak y este después de verificar presenta una pantalla donde se solicita al usuario realizar una prueba de vida, luego se procede a la verificación de la prueba y el servidor de keycloak retorna los tokens que van a servir para la comunicación continua del sistema segurizado durante la interacción del usuario como se muestra en el flujo de la Figura 16.

Figura 16

Proceso de login con keycloak y prueba de vida



Metodología de investigación

Para el proyecto de investigación se utilizó un conjunto de procesos basados en el método científico experimental relacionado directamente a la Inteligencia Artificial, se buscó modelos que se adecúen a los requerimientos del cliente, adquiriendo los conocimientos necesarios para generar la solución propuesta en este documento.

Esta metodología se caracteriza por el hecho de que los investigadores pueden controlar deliberadamente las variables para delimitar las relaciones entre ellas. Estas variables pueden ser dependientes o independientes, siendo fundamentales para recopilar los datos que se extraen de un grupo experimental, así como su comportamiento. Esto permite descomponer los procesos conscientes en sus elementos, descubrir sus posibles conexiones y determinar las leyes de esas conexiones. (investigacioncientifica.org, 2022).

El método científico experimental presenta una serie de pasos que permitió el desarrollo de la solución propuesta en este documento, en la Tabla 5 se mencionan los pasos que sirvieron de guía dentro del desarrollo propuesto.

Tabla 5

Pasos del método científico experimental

Paso	Descripción
1.- Observaciones	Las observaciones deben ser verificables
2.- Hipótesis	El principio general se llama hipótesis. El tipo de razonamiento involucrado se denomina razonamiento inductivo (derivación de una generalización a partir de detalles específicos).
3.- Predicción	La hipótesis debe ser amplia y debe aplicarse uniformemente a través del tiempo y el espacio. Los científicos generalmente no pueden verificar todas las situaciones posibles en las que se puede aplicar una hipótesis.
4.- Experimento	Se diseña un experimento basado en la predicción
5.- Análisis	Se realiza el análisis de los resultados del experimento diseñado en el paso anterior
6.- Conclusión	Se determina si el experimento coincide con la predicción o es contraria, a partir de aquí el investigador vuelve a realizar los pasos

Paso	Descripción
	mencionados para obtener más datos y diversos diseños del experimento
7.- Resultados	Los científicos publican sus hallazgos en revistas científicas y libros, en conversaciones en reuniones nacionales e internacionales y en seminarios en colegios y universidades.

Nota. Tomado de Extracto propio tomado de https://investigacioncientifica.org/que-es-el-metodo-cientifico-experimental/

Capitulo II

Diseño del sistema

La especificación de requerimientos es uno de los pasos fundamentales para empezar con el desarrollo de la solución propuesta en este documento, en este capítulo se estructuraron dichas especificaciones partiendo de los pedidos del cliente, además del diseño de los modelos de casos de uso, que ayudaron como guía y constancia durante la ejecución del proyecto, la solución propuesta se implementó de manera adecuada al flujo de login que tiene la corporación favorita.

Se tomó como guía el método científico experimental, esto permitió ir generando nuevos alcances en el desarrollo de la solución propuesta en este documento al igual que generó la filtración de diversos modelos de inteligencia artificial que se adecuen al requerimiento planteado, el requerimiento fue la implementación de un login en keycloak con reconocimiento facial que permita realizar una prueba de vida, en la

Tabla 6

Tareas involucradas en la solución propuesta

Tarea	Descripción
Detección de rostro	En esta tarea se realizó la evaluación de diferentes modelos de inteligencia artificial que permitan detectar rostros en una imagen input
Reconocimiento del rostro identificado	En esta tarea se realizó la evaluación de diferentes técnicas para que el rostro detectado

Tarea	Descripción
	con los modelos de la tarea anterior pueda ser identificados y asociados a una persona, hubo problemas de escalabilidad en las pruebas por lo que estas técnicas se descartaron para una primera versión de la solución, sin embargo, están planteadas para mejorar una siguiente entrega.
Detección de posición del rostro (perfiles)	En esta tarea se realizó la búsqueda de diferentes modelos de inteligencia artificial que permitan detectar la posición en la que se encuentran los rostros previamente detectados en la primera tarea.
Detección de pestañeo	En esta tarea se realizó la búsqueda de diferentes modelos de inteligencia artificial que permitan detectar en una imagen si el rostro detectado tiene los ojos cerrados o abiertos, por lo cual al implementarlo en un flujo de tiempo se puede determinar si el rostro detectado genera la acción de pestañear.
Identificación de emociones	En esta tarea se realizó la búsqueda de diferentes modelos de inteligencia artificial que permitan la identificación de emociones en un rostro previamente detectado en la primera tarea.

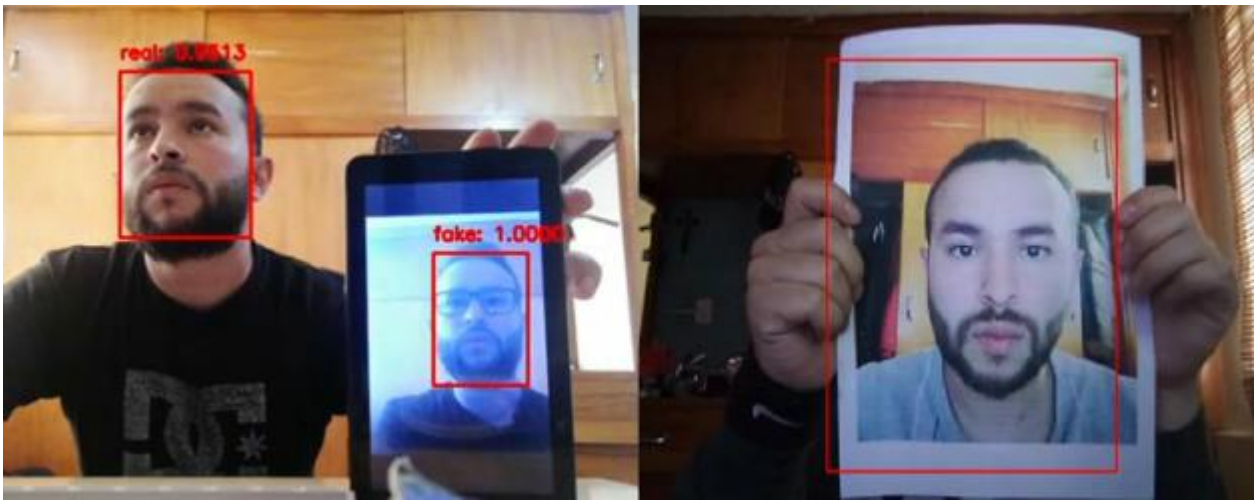
Tarea	Descripción
Identificación de género	
Estimación de edad	En esta tarea se realizó la búsqueda de diferentes modelos de inteligencia artificial que permitan la estimación de edad en un rostro previamente detectado en la primera tarea. Los pocos modelos que se encontraron presentaron diferentes estimaciones para un mismo rostro en diversas ejecuciones, por lo cual no se pudo tener consistencia en los resultados y se descartaron la utilización de estos modelos.
Estimación de raza	En esta tarea se realizó la búsqueda de diferentes modelos de inteligencia artificial que permitan la estimación de raza en un rostro previamente detectado en la primera tarea. Los pocos modelos que se encontraron presentaron diferentes estimaciones para un mismo rostro en diversas ejecuciones, por lo cual no se pudo tener consistencia en los resultados y se descartaron la utilización de estos modelos.
Extensión de funcionalidades en Keycloak	En esta tarea se realizó la lectura de la documentación del proveedor de identidades Keycloak, para poder programar una extensión de

Tarea	Descripción
	funcionalidades que van a servir para integrar al flujo de login el consumo del API para las pruebas de vida.
Detección de fraude (Videos en dispositivos e impresiones)	En esta tarea se realizó una búsqueda de diferentes modelos de inteligencia artificial que permitan identificar si el rostro detectado en la primera tarea es un input directamente desde la cámara del usuario o por el contrario es un input que proviene de un Spoofing ya sea por rostro impreso en hoja o un rostro presentado en un dispositivo móvil. La ejecución del modelo encontrado fue bastante pesada por lo cual el rendimiento del sistema en general decaía muchísimo. Por lo cual este modelo fue descartado hasta realizar los entrenamientos necesarios para optimizar la ejecución del mismo y poder integrarlo en futuras versiones del sistema. En la Figura 17 se puede visualizar el resultado del modelo.
Challenge (Liveness Proof) con modelos evaluados en el lado del servidor	En esta tarea se realizó el desarrollo del banco de preguntas en el cual se llaman a los

Tarea	Descripción
	modelos investigados en las tareas anteriores y se procede a evaluar la prueba de vida.

Figura 17

Ejemplo de modelo de detección de fraude



Problemática y modelo de solución

Al existir una gran cantidad de sistemas que requieren el acceso de usuarios y al tener un proveedor de identidades y accesos centralizado como keycloak, fue importante implementar la solución sin que afecte todas estas condiciones, para lo cual, se analizó la factibilidad de una arquitectura de microservicios, ya que nos permite aislar el sistema de prueba de vida, y hacer uso del mismo mediante comunicación directa con el servidor de keycloak.

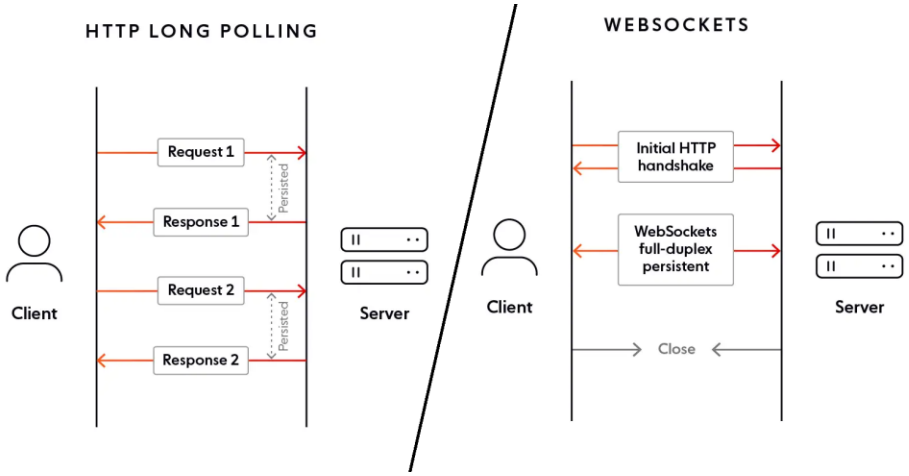
Especificación de protocolos de comunicación

Se analizó el sistema de comunicación adecuado para implementar en la solución a la problemática de este proyecto de investigación “sistema de prueba de vida para login biométrico usando modelos de machine learning”, se determinó que el mejor protocolo para utilizar es de websockets, ya que, se requiere que la prueba de vida sea en tiempo real al momento de realizar el login en cualquier sistema segurizado con keycloak en la Figura 18

Protocolos Http vs WebSocketsFigura 18 se observa la diferencia entre los dos protocolos.

Figura 18

Protocolos Http vs WebSockets



Nota. Tomado de https://ably.com/topic/websockets-vs-http

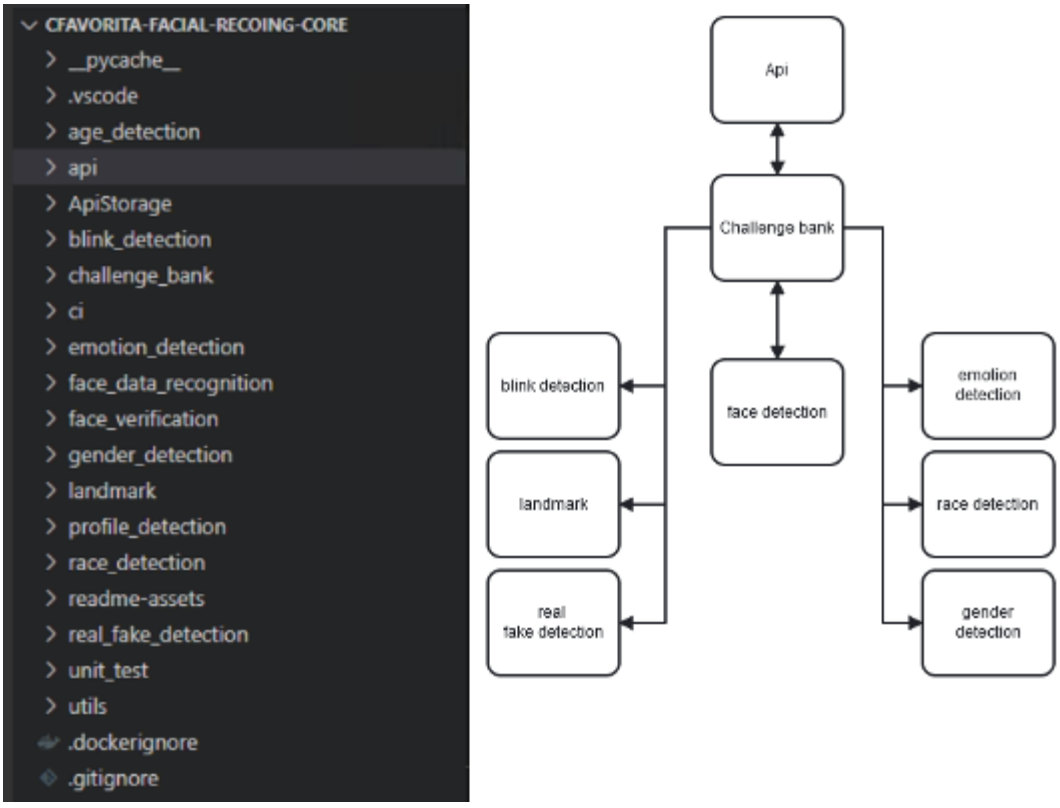
Arquitectura del sistema de prueba de vida

La arquitectura seleccionada para el microservicio fue modular, pudiendo agregar o quitar módulos de los modelos de Inteligencia artificial usados de una forma relativamente sencilla y sin afectar la funcionalidad de los otros módulos, como se aprecia en la Figura 19. A nivel de código se tiene la exposición de los servicios mediante una API, esta se comunica con el módulo que realiza todas

las preguntas aleatorias que es el challenge_bank, en este módulo es el que se genera toda la lógica de la prueba de vida y este módulo hace el uso de los demás módulos que trabajan independientemente con sus respectivos modelos de Inteligencia Artificial.

Figura 19

Arquitectura modular



En caso de requerir o encontrar nuevas formas para mejorar o incrementar la prueba de vida se puede agregar un módulo con el respectivo modelo de inteligencia artificial y programar la lógica de consumo en el módulo challenge_bank.

Módulo de banco de preguntas (challenge_bank)

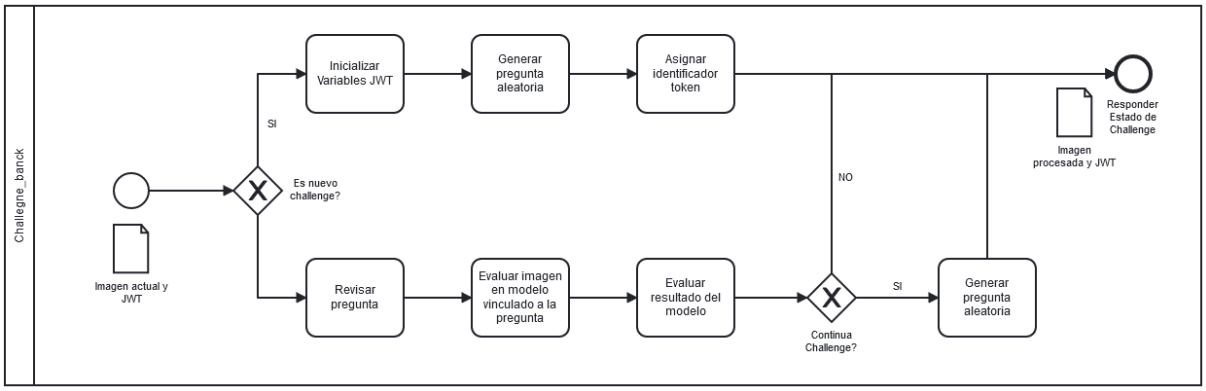
Este módulo fue el más complicado de diseñar, ya que los requerimientos de temporalidad, es decir, que una prueba de vida no es simplemente evaluar una imagen, sino el evaluar un flujo de imágenes en un determinado lapso de tiempo, y la comunicación en tiempo real para efectuar esta acción, representó un gran reto.

Este módulo consistió en desarrollar un generador de acciones aleatorias que debe realizar el usuario, cada una de estas acciones o preguntas están vinculadas con un modelo de inteligencia artificial, por ejemplo, si la acción que se le solicita al usuario es parpadear, esta acción está vinculada al módulo con el modelo de inteligencia artificial que verifica si en la imagen se realizaron parpadeos o no, igualmente si la acción que se le solicita al usuario es sonreír, esta acción va a ser evaluada en el módulo de detección de emociones.

Para mantener la consistencia en la prueba de vida se hacen uso de una serie de variables que viajan tokenizadas en la conexión websocket como se puede observar en la Figura 20.

Figura 20

Proceso del módulo del banco de preguntas



En Tabla 7 se describen los modelos de inteligencia artificial y las acciones relacionadas a las mismas que se utilizaron en la solución de la problemática de este proyecto de investigación “sistema de prueba de vida para login biométrico usando modelos de machine learning”.

Tabla 7

Modelos utilizados en el banco de preguntas

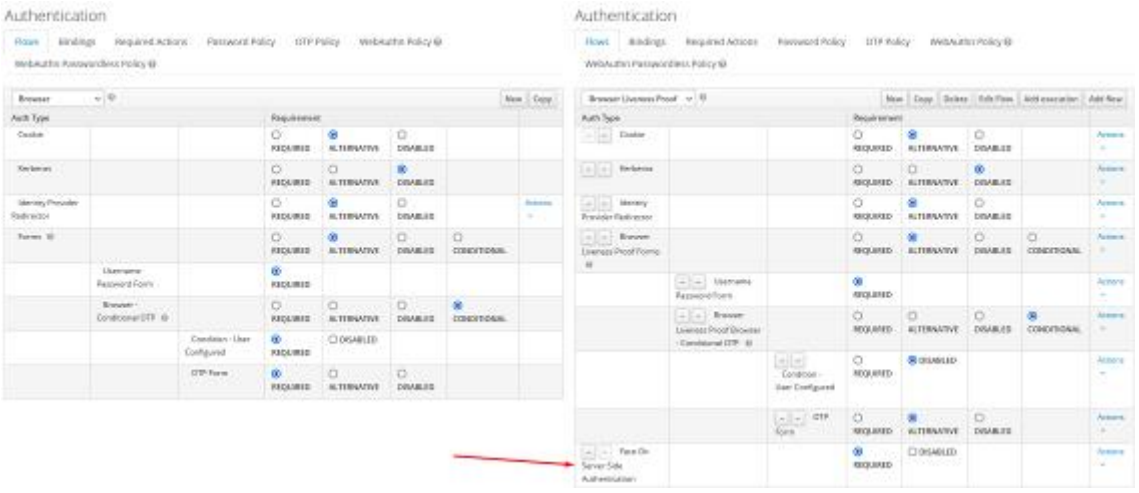
Modelo	Acciones requeridas
Detección de perfiles	Cuando se pide que el usuario gire su cabeza a la izquierda o a la derecha
Detección de parpadeo	Cuando se pide que el usuario parpadee consecutivamente
Detección de emociones	Cuando se pide que el usuario represente una emoción, en este caso se solicita al usuario sonreír

Extender funcionalidades de Keycloak

Siguiendo la documentación de keycloak y al ser un sistema de código abierto, esto permitió generar un proyecto para poder extender las funcionalidades del proveedor de identidades Keycloak. Este proyecto es un SPI (Service Provider Interfaces) personalizado, lo cual permitió agregar a los flujos de login un paso adicional para configuración de la prueba de vida como segundo factor de autenticación, como se ejemplifica en la Figura 21 al lado izquierdo se muestra la configuración de flujo por defecto en keycloak y al lado derecho se muestra la misma configuración, pero se agrega el paso adicional de la prueba de vida.

Figura 21

Extensión de funcionalidad del flujo de login web en keycloak



Capítulo III

En capítulos previos se definió la mejor arquitectura y se explicó el uso de cada componente para que el sistema de prueba de vida cumpla con el requerimiento de la Corporación Favorita, por lo que en este capítulo se puso en práctica el prototipo planteado y se exponen los resultados para que estos puedan ser revisados de tal manera que en un futuro se pueda o no pensar en una implementación en el ambiente de producción.

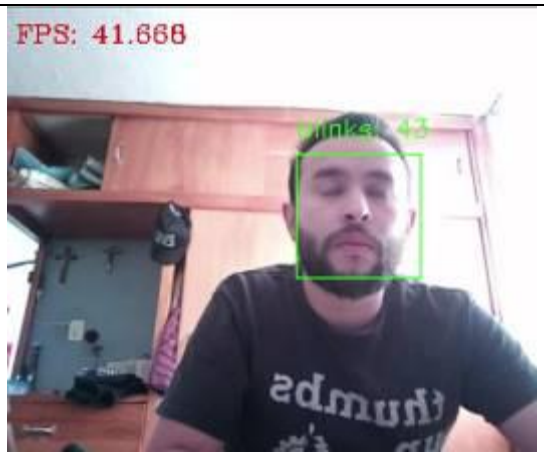
Implementación y pruebas

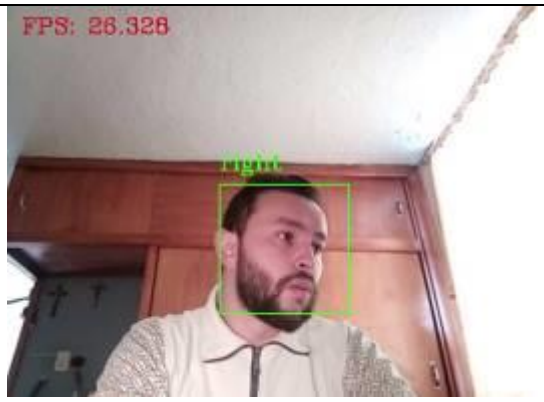
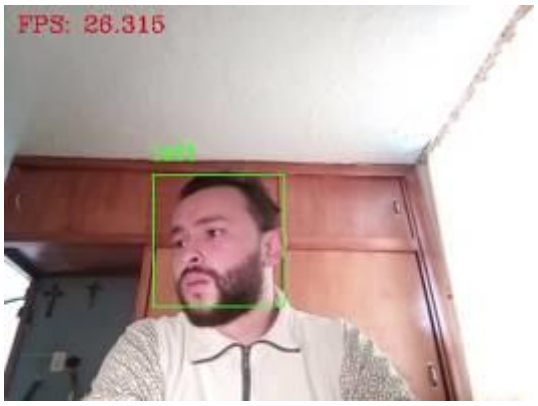
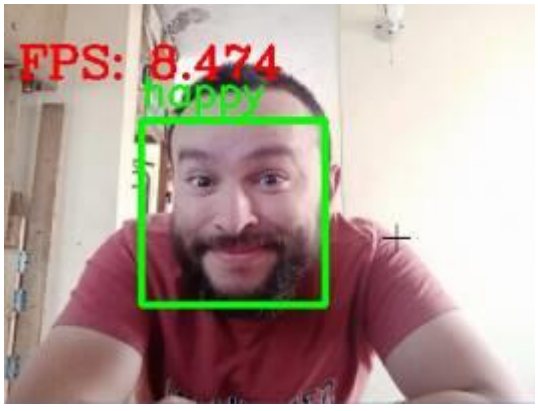
Implementación de los modelos

Antes de que todo el sistema de prueba de vida funcione como un todo, se realizaron pruebas de cada modelo que se utilizó en la solución de este proyecto de investigación. En la Tabla 8 se presentan de manera visual los resultados de cada modelo.

Tabla 8

Resultados de cada modelo de inteligencia artificial de manera individual

Resultado modelo	Descripción
	El modelo de parpadeo permite contar los parpadeos que realiza el usuario. De aquí se puede pedir que el usuario parpadee. Es un modelo que se ejecuta bastante rápido debido a que hace uso de Landmarks.

Resultado modelo	Descripción
	El modelo de posición del rostro es eficiente, hace uso de un clasificador de rostros proporcionado por OpenCV, este modelo solo se activa si el rostro está mirando a la derecha.
	Es el mismo modelo clasificador de rostros proporcionado por OpenCV, sin embargo, como este modelo solo se activa si el rostro está mirando a la derecha, previamente hay que girar la imagen en espejo de manera vertical, para que de esta manera el lado izquierdo se muestre como derecho y se active el modelo.
	La detección de emociones es el más lento de todos. Ya que es un modelo de Deep learning y sus inferencias son más demorosas si se trabajan en entornos que carecen de tarjetas gráficas Nvidia.

Implementación del banco de preguntas

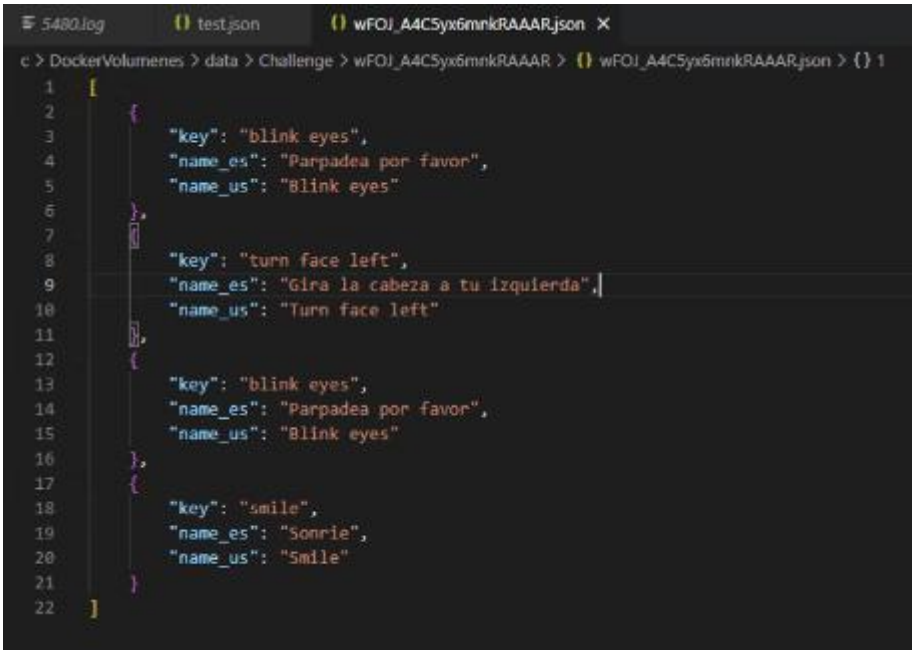
Para probar el banco de preguntas se realizaron la compilación de los resultados del Challenge en un archivo JSON en el cual se muestran las preguntas aleatorias que se presentaron al usuario, esto

con el fin de comprobar que el Challenge se efectuó correctamente como se muestra en la Figura 22

Ejemplo de preguntas aleatorias generadas por el banco de preguntas Figura 22.

Figura 22

Ejemplo de preguntas aleatorias generadas por el banco de preguntas



Evaluación de resultados

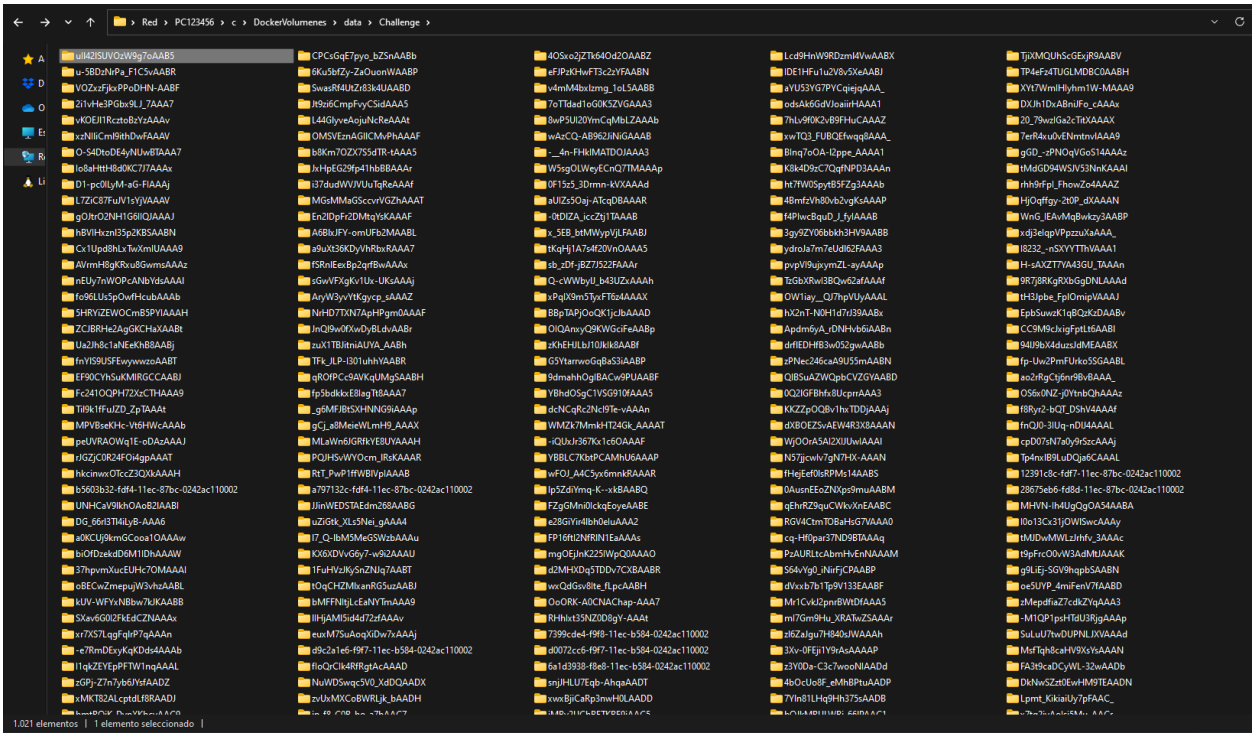
Una vez integrados los diferentes modelos de inteligencia artificial al flujo del banco de preguntas se realizaron evaluaciones en un html que realiza la petición de una prueba de vida en modo debug para revisar que la pregunta y los parametros de evaluación de la misma sean los correctos como se puede observar en la Figura 23, adicional a eso el sistema guarda cada prueba de vida en directorios para poder realizar auditorias aleatorias como se muestra en la Figura 24.

Figura 23

Evaluación de prueba de vida en modo debug

Figura 24

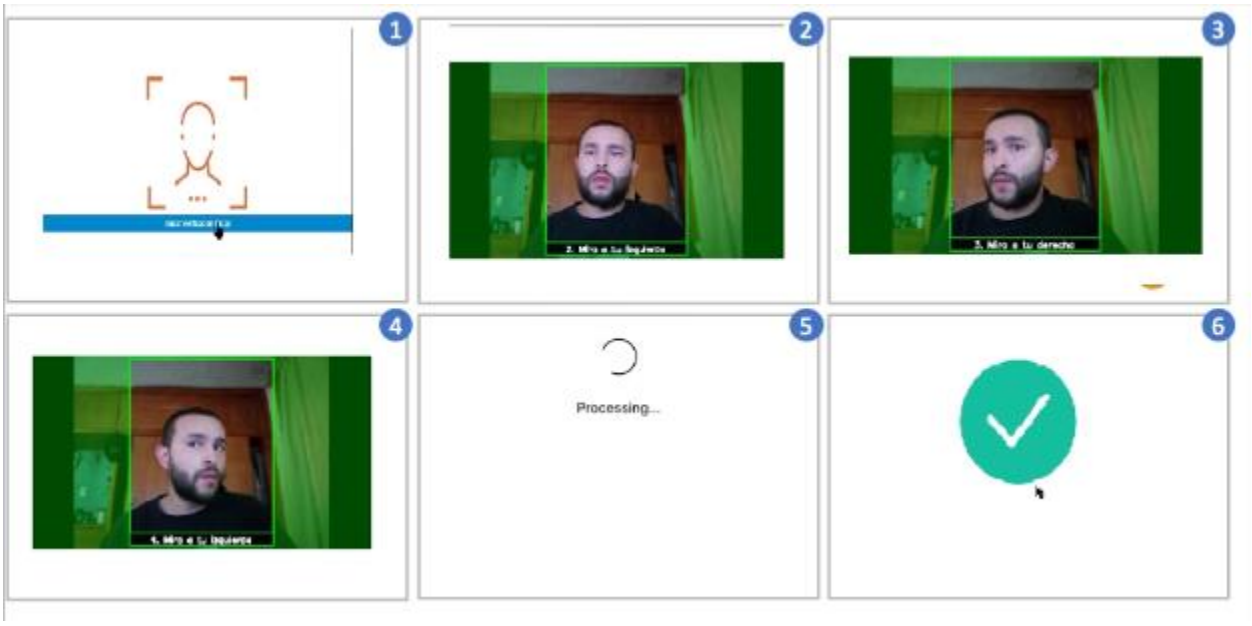
Pruebas realizadas



En la Figura 25 se observa un ejemplo exitoso de los pasos que el sistema de prueba de vida realiza para poder validar el acceso a cualquier sistema que se encuentre segurizado con keycloak, describiendo paso uno se muestra la pantalla donde se va a dar inicio a la prueba de vida, paso dos recibe la primera acción de mirar a la izquierda, al validar esta acción se genera una segunda pregunta en el paso tres que en este caso es mirar a la derecha, al validar esta acción se genera una tercera pregunta en el paso cuatro que en este caso es volver a mirar a la izquierda, como ha respondido exitosamente las tres primeras preguntas se muestra la validación en el paso cinco y posterior aprobación en el paso seis, con lo cual se permite el ingreso al sistema segurizado.

Figura 25

Ejemplo de prueba de vida exitoso integrado en login



Capítulo IV

En este Capítulo se detallan las conclusiones y recomendaciones del presente proyecto, esto se lo realizó partiendo de los objetivos establecidos al inicio del mismo. Las recomendaciones se centraron en los problemas que se encontraron durante el desarrollo del sistema, además de que puede servir como ayuda para futuros proyectos relacionados al tema.

Conclusiones y líneas de trabajo futuro

Conclusiones

- No se encontró diferencia significativa entre estos modelos, por lo cual, la utilización de cualquiera de los mencionados en este documento puede ser sostenible para la solución propuesta.
- La mejor opción fue utilizar una comunicación websocket bidireccional entre el cliente y el servidor, ya que la propuesta de solución requería un canal de comunicación en tiempo real.
- La solución propuesta fue diseñada para integrarse correctamente al proveedor de identidades keycloak.
- Se realizaron pruebas satisfactorias sobre el sistema y la integración en el flujo de login web de aplicaciones segurizadas de Corporación Favorita.

Recomendaciones

- Para integrar diferentes modelos de inteligencia artificial hay que tener en cuenta la forma peculiar de utilizar cada uno de esos modelos, y estandarizar el consumo usando patrones estructurales como el Adapter que permite la colaboración entre objetos con interfaces incompatibles.

- Para una efectiva ejecución de la solución propuesta en este documento se recomienda la utilización de hardware acelerado por tarjetas gráficas porque permiten la paralelización de las inferencias requeridas de diferentes modelos de inteligencia artificial.

Bibliografía

Agarval, V. (2022). *towardsdatascience.com*. Obtenido de Face Detection Models: Which to Use and Why?: https://towardsdatascience.com/face-detection-models-which-to-use-and-why-d263e82c302c

Ali, Z., & Park, U. (2019). Face Spoofing Attack Detection Using Spatial Frequency and Gradient-Based Descriptor. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 13, NO. 2, Feb. 2019* .

Amador Hidalgo, L. (1996). *Inteligencia artificial y sistemas expertos.* Obtenido de Universidad de Córdoba, Servicio de Publicaciones: https://helvia.uco.es/handle/10396/6938

Ambalakat, P. (2009). Security of Biometric Authentication Systems. *Computer Science Semina*.

Arthur, S. (1959). Pionero en el campo del aprendizaje automático (ML).

Berle, I. (2020). *Face Recognition Technology Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images.* Switzerland : Springer Nature Switzerland AG 2020.

Besnassi, M., Neggaz, N., & Benyettou , A. (14 de 02 de 2019). *SpringerLink*. Obtenido de Face detection based on evolutionary Haar filter: https://link.springer.com/article/10.1007/s10044-019-00784-5

Bhattacharjee, S., Mohammadi, A., & Marcel, S. (2018). Spoofing Deep Face Recognition with Custom Silicone Masks.

Biometrics Institute Limited. (s.f.). What does presentation attack detection and liveness actually mean? *Biometrics Institute*.

Boden, M. (1984). *Inteligencia artificial y hombre natural .* Obtenido de https://papers.uab.cat/article/view/v24-elejebarrieta

Bourlai, T., Karampelas, P., & Patel, V. M. (2020). *Securing Social Identity in Mobile Platforms Technologies for Security, Privacy and Identity Management.* Switzerland : Springer Nature Switzerland AG 2020.

Bowyer, K. W., & Burge, M. J. (2016). *Handbook of Iris Recognition.* London : Springer-Verlag London 2013, 2016.

Braga-Neto, U. (2020). *Fundamentals of Pattern Recognition and Machine Learning.* Switzerland : Springer Nature Switzerland AG 2020 .

C H Chen University of Massachusetts Dartmouth, USA. (2020). *HANDBOOK OF PATTERN RECOGNITION AND COMPUTER VISION 6th Edition.* Singapore: World Scientific Publishing Co. Pte. Ltd.

Chen, L., Wu, M., Pedrycz, W., & Hirota, K. (2021). *Emotion Recognitio and Understanding for Emotional Human-Robot Interaction Systems.* Switzerland: Springer Nature Switzerland AG 2021.

Chingovska, I., Anjos, A., & Marcel, S. (2012). On the Effectiveness of Local Binary Patterns in Face Anti-spoofing. *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*.

Chingovska, I., Mohammadi, A., Anjos, A., & Marce, S. (s.f.). Evaluation Methodologies for Biometric Presentation Attack Detection.

Costa-Pazo, A., Bhattacharjee, S., Vazquez-Fernandez, E., & Marcel, S. (s.f.). The REPLAY-MOBILE Face Presentation-Attack Database.

Delac, K., Grgic, M., & Bartlett, M. S. (2008). *Recent Advances in Face Recognition.* Croatia: In-Te.

Delac, K., Grgic, M., & Bartlett, M. S. (2008). *Recent Advances In Face Recognition.* Croatia: In-Teh. Obtenido de https://books.google.com.ec/books?id=6DehDwAAQBAJ&lpg=PA109&ots=POdW3WfLa-&dq=liveness%20detection%20biometric%20authentication&lr&hl=es&pg=PA111#v=onepage&q=liveness%20detection%20biometric%20authentication&f=false

Distante, A., & Distante, C. (2020). *Handbook of Image Processing and Computer Vision Volume 1: From Energy to Image.* Switzerland : Springer Nature Switzerland AG 2020.

Distante, A., & Distante, C. (2020). *Handbook of Image Processing and Computer Vision Volume 2: From Image to Pattern.* Switzerland : Springer Nature Switzerland AG 2020.

Distante, A., & Distante, C. (2020). *Handbook of Image Processing and Computer Vision Volume 3: From Pattern to Object.* Switzerland : Springer Nature Switzerland AG 2020.

Docker. (s.f.). *Docker*. Obtenido de Docker: https://www.docker.com/

Dutta, P., & Barman, A. (2020). *Human Emotion Recognition from Face Images.* Singapore : Springer Nature Singapore Pte Ltd. 2020.

Erdogmus, N., & Marcel, S. (2013). Spoofing in 2D Face Recognition with 3D Masks and Anti-spoofing with Kinect. *IEEE*, Idiap Research Institute.

GALBALLY, J., MARCEL, S., & FIERREZ, J. (2015). Biometric Antispoofing Methods: A Survey in Face Recognition. *IEEE Access*.

Ghaffar, I. A., & Mohd, M. N. (2021). Presentation Attack Detection for Face Recognition on Smartphones: A Comprehensive Review. *Journal of Telecommunication, Electronic and Computer Engineering*, 33 - 38 .

Hagemann, S., Sunnetcioglu, A., & Stark, R. (2019). Hybrid Artificial Intellegence System for the Design of Highly Automated Production Systems. *ScienceDirect*, 160 - 166.

Hands-On Transfer Learning with Python. (2018). Birmingham: Packt Publishing Ltd.

investigacioncientifica.org. (2022). *investigacioncientifica.org*. Obtenido de https://investigacioncientifica.org/que-es-el-metodo-cientifico-experimental/

Jayaraman, U., Gupta, P., Gupta, S., Arora, G., & Tiwari, K. (2020). Recent development in face recognition. *ScienceDirect*, 231 - 245.

Jiang, R., Li, C.-T., Crookes, D., Meng, W., & Rosenberger, C. (2020). *Deep Biometrics.* Switzerland: Springer Nature Switzerland AG 2020.

Jiang, X., Hadid, A., Pang, Y., Granger, E., & Fen, X. (2019). *Deep Learning in Object Detection and Recognitio.* Singapore : Springer Nature Singapore Pte Ltd. 2019.

Khanna, A., Gupta, D., Bhattacharyya, S., Snasel, V., Platos, J., & Hassanien, A. E. (2019). *International Conference on Innovative Computing and Communications.* Singapore : Springer Nature Singapore Pte Ltd. 2020.

Kleinig, J., Mameli, P., Miller, S., Salane, D., & Schwartz, A. (2011). *SECURITY and PRIVACY Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States.* Canberra: ANU E Press.

kubernetes. (21 de 09 de 2021). Obtenido de Qué es Kubernetes: https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/

Le Cun, Boser, Denker, Henderson, Howard, Hubbard, & Jackel. (s.f.). *Handwritten Digit Recognition with a Back-Propagation Network*. Obtenido de https://proceedings.neurips.cc/paper/1989/file/53c3bce66e43be4f209556518c2fcb54-Paper.pdf

Li, S. Z., & Jain, A. K. (2011). *Handbook of Face Recognition.* London : Springer-Verlag London Limited 2011.

Marcel, S., Nixon, M. S., Fierrez, J., & Evans, N. (2019). *Handbook of Biometric Anti-Spoofing Presentation Attack Detection.* Switzerland : Springer Nature Switzerland AG 2019.

Michelucci, U. (2019). *Advanced Applied Deep Learning Convolutional Neural Networks and Object Detection.* Switzerland.

OpenCV. (2022). *GitHub*. Obtenido de Haarcascades: https://github.com/opencv/opencv/tree/master/data/haarcascades

Owczarek, A., & Ślot, K. (0212). Lipreading Procedure for Liveness Verification in Video Authentication Systems. *Institute of Electronics, Technical University of Lodz*, 115 - 124 .

Peixoto, B., Michelassi, C., & Rocha, A. (2011). FACE LIVENESS DETECTION UNDER BAD ILLUMINATION CONDITIONS. *University of Campinas (Unicamp)*.

Python. (21 de 09 de 2021). *Python*. Obtenido de https://www.python.org/

Rattani, A., Derakhshani, R., & Ross, A. (2019). *Selfie Biometrics Advances and Challenges.* Switzerland : Springer Nature Switzerland AG 2019.

Rouhiainen, L. (2018). *Lasse Rouhiainen.* Obtenido de planetadelibros: https://www.planetadelibros.com/libros_contenido_extra/40/39307_Inteligencia_artificial.pdf

Sánchez-Sánchez, M. A., Conde, C., Gómez-Ayllón, B., Ortega-DelCampo, D., Tsitiridis, A., Palacios-Alonso, D., & Cabello, E. (2020). Convolutional Neural Network Approach for Multispectral Facial Presentation Attack Detection in Automated Border Control Systems. *Entropy*, 2- 18.

Santana Vega, C. (s.f.). Divulgador de inteligencia Artificial. España.

Schuckers, S. (2016). Presentations and Attacks, and Spoofs, Oh My. *Image*, 26 - 30.

Scrivener, M., & Carmical, P. (2021). *Recognition and Perception of Images.* Beverly: Scrivener Publishing.

Shelton, J., Roy, K., O'Connor, B., & Dozier, G. V. (2014). Mitigating Iris-Based Replay Attacks. En *International Journal of Machine Learning and Computing, Vol. 4, No. 3* (págs. 204 - 209).

Solano, G. (s.f.). *Omes*. Obtenido de https://omes-va.com

Subramanian, V. (2018). *Deep Learning with PyTorc.* Birmingham: Packt Publishing Ltd.

Torrubia, A. (s.f.). Divulgador de Inteligencia Artificial.

Tussy, K. A., Wojewidka, J., & Rose, J. (14 de 05 de 2021). *Liveness.com*. Obtenido de Biometric Liveness Detection Explained: https://liveness.com/

Tussy, K., Wojewidka, J., & Josh Rose. (21 de 09 de 2021). *liveness*. Obtenido de https://liveness.com/

Vento, M., & Percannella, G. (2019). *Computer Analysis of Images and Patterns Part 1.* Switzerland: Springer Nature Switzerland.

Vento, M., & Percannella, G. (2019). *Computer Analysis of Images and Patterns Part 2.* Switzerland: Springer Nature Switzerland.

Viola, P., & Jones, M. (2001). *Rapid Object Detection using a Boosted Cascade of Simple*. Obtenido de Rapid Object Detection using a Boosted Cascade of Simple: https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf

w3schools. (21 de 09 de 2021). *HTML*. Obtenido de w3schools: https://www.w3schools.com/html/default.asp

Zafar, I., Tzanidou, G., Burton, R., Patel, N., & Araujo, L. (2018). *Hands-On Convolutional Neural Networks with TensorFlow.* Birmingham: Packt Publishing Ltd.